

Министерство образования и науки Российской Федерации
ФГБОУ ВО «Уральский государственный педагогический университет»
Институт математики, информатики и информационных технологий
Кафедра высшей математики

Использование прикладного пакета GAP для описания решеток подалгебр четырехмерных алгебр над полем $GF(2)$

Выпускная квалификационная работа

Квалификационная работа
допущена к защите
Зав. кафедрой

дата подпись

Исполнитель:
Гусельникова Татьяна Станиславовна,
обучающаяся БП-41 группы

подпись

Руководитель ОПОП:

подпись

Научный руководитель:
Коробков С.С.,
к.ф.-м.н., доцент

подпись

Екатеринбург 2016

Оглавление

Введение	3
ГЛАВА I. Теоретические основы	6
1.1. Основные понятия	6
1.2. Алгебраические элементы колец	7
1.3. Пирсовские разложения колец	8
1.4. Понятие алгебры над полем	10
1.5. Алгебра матриц над конечным полем	10
1.6. Понятие подалгебры. Признак подалгебры	11
1.7. Изоморфизм алгебр	11
1.8. Понятие решетки. Основные свойства решеток	14
1.9. Диаграммы решеток	16
1.10. Решетка подалгебр алгебры над полем	17
ГЛАВА II. Система компьютерной алгебры GAP	19
2.1. Общая характеристика пакета GAP	19
2.2. Язык программирования GAP	21
2.3. Общие команды пакета	22
2.4. Команды для вычисления в алгебрах	24
ГЛАВА III. Типовая классификация подалгебр четырехмерной алгебры матриц $M(GF(2),3)$	26
3.1. Типы решеток подалгебр четырехмерных алгебр	26
3.2. Подалгебры, имеющие решетку типа $(1, 11, 17, 7, 1)$	26
3.3. Классификация четырехмерных подалгебр в алгебре матриц третьего порядка над полем из двух элементов	36
Литература	43
Приложение 1	44
Приложение 2	59
Приложение 3	61
Приложение 4	63
Приложение 5	64
Приложение 6	65
Приложение 7	66
Приложение 8	67

Введение

Матричные алгебры играют большую и важную роль в теории ассоциативных алгебр, в связи с этим возникает большой интерес к их исследованию. Уникальность матричной алгебры подтверждается и тем, что она определяется своей решеткой подалгебр, то есть каждая алгебра, решеточно изоморфная алгебре матриц $A = M_n(F)$, где $n > 1$, изоморфна A . Решетка подалгебр алгебры A в свою очередь является богатым источником решеток подалгебр конечномерных алгебр ввиду того, что каждая конечномерная алгебра изоморфно вкладывается в соответствующую алгебру матриц [12].

В данной работе рассматривается алгебра квадратных матриц порядка 3 над полем из двух элементов и ее подалгебры. Ранее в работе [11] были найдены все подалгебры алгебры A . Их количество оказалось равным числу 2102. Кроме того, были найдены и типы решеток подалгебр для всех подалгебр. Число типов решеток равно 30. Определим тип решетки подалгебр:

Определение 1. Пусть S – подалгебра порядка 2^n алгебры $M_3(GF(2))$. Назовем упорядоченную последовательность (m_0, m_1, \dots, m_n) *типом* решетки подалгебр алгебры S , если m_i – число подалгебр в S порядка 2^i .

Дальнейшие исследования могут быть направлены на решение вопроса об изоморфизме решеток, имеющих один и тот же тип. Если две подалгебры из A имеют решетки подалгебр одного типа, а сам тип достаточно простой, то легко устанавливается изоморфизм между решетками их подалгебр.

Основная цель работы состоит в описании решеток подалгебр четырехмерных алгебр, содержащихся в алгебре A .

Описание решетки подалгебры сводится к нахождению всех элементов решетки и к определению отношения между ними. Затем изображается диаграмма самой решетки. Для достижения основной цели решаются следующие задачи:

1. Строятся четырехмерные подалгебры алгебры A .

2. Определяются типы решеток подалгебр четырехмерных алгебр.
3. Выбирается конкретный тип решетки, и находятся определяющие соотношения элементов, порождающих данную подалгебру S .
4. Находятся все подалгебры алгебры A , изоморфные подалгебре S .
5. Строится решетка подалгебр алгебры S .

Решение данных задач осуществляется с помощью компьютерного пакета GAP.

Работа состоит из введения, трех глав, списка литературы и приложения. Основное содержание работы изложено в трех главах. Первая глава служит базой, в которой вводятся понятия основных алгебраических структур (группа, кольцо, поле, алгебра над полем), рассматриваются идемпотентные и нильпотентные элементы, пирсовские разложения, подалгебры матричных алгебр, начальные понятия теории решеток.

Вторая глава посвящена системе компьютерной алгебры GAP, ее характеристикам, особенностям и основным командам для вычисления в алгебрах. Данная система GAP является некоммерческим, свободным, открытым и расширенным пакетом программного обеспечения для вычислений в дискретной (абстрактной) алгебре.

Практическая часть представлена в третьей главе. В ней приводятся результаты исследований с выбранными типами решеток. Для этого составляются программы в системе компьютерной алгебры GAP и приводится их описание.

Получены следующие результаты:

Теорема 1. В алгебре A существует всего 84 подалгебры с решеткой типа $(1, 8, 12, 6, 1)$. Все эти подалгебры разбиваются на 2 подмножества, содержащих по 42 подалгебре. В каждом классе все подалгебры изоморфны между собой, а значит, имеют изоморфные решетки подалгебр, а подалгебры их различных классов – не изоморфны.

Теорема 2. В алгебре A существует всего 14 подалгебр с решеткой типа $(1, 7, 11, 1, 1)$. Все эти подалгебры изоморфны между собой, а значит, имеют изоморфные решетки подалгебр.

В работе проводилось исследование подалгебр, имеющих решетку типа $(1, 11, 17, 7, 1)$. Исследовано 2 класса подалгебр такого типа (в каждом классе по 14 подалгебр) и найдены решетки подалгебр в каждом классе. Также исследовались подалгебры, имеющие решетку типа $(1, 12, 20, 9, 1)$. Найден 1 класс состоящий из 10 подалгебр. Все эти подалгебры изоморфны между собой и имеют одну и ту же решетку подалгебр.

ГЛАВА I. Теоретические основы

1.1. Основные понятия

Определение 1. Непустое множество M элементов произвольной природы (например, чисел, отображений, преобразований) называется *группой*, если выполняются четыре следующих условия.

1. Задан закон композиции, который каждой паре элементов a и b из M сопоставляет третий элемент этого же множества, называемый, произведением элементов a и b и обозначаемый через ab .
2. Закон ассоциативности. Для любых трех элементов a, b, c из M имеет место равенство $(ab)c = a(bc)$.
3. В M существует (левая) единица e , т. е. элемент e , выделяемый следующим свойством: $ea = a$.
4. Для каждого элемента a из M существует (по крайней мере) один (левый) обратный элемент a^{-1} в M , определяемый свойством: $a^{-1}a = e$.

Определение 2. Группа называется *абелевой*, если, кроме того, оказывается выполненным тождество $ab = ba$ (закон коммутативности).

Определение 3. Для того чтобы непустое подмножество W данной группы M было *подгруппой*, необходимо и достаточно выполнение следующих условий:

1. Множество W содержит вместе с любыми двумя своими элементами и их произведение.
2. Множество W содержит вместе с каждым своим элементом a обратный к нему элемент a^{-1} .

Определение 4. Множество R называется *кольцом*, если операции над элементами подчиняются следующим законам:

1. Законы сложения:
 - а) Закон ассоциативности: $a + (b + c) = (a + b) + c$;
 - б) Закон коммутативности: $a + b = b + a$;

в) Разрешимость уравнения для всех a, b .

2. Закон умножения:

а) Закон ассоциативности: $a(bc) = (ab)c$;

3. Законы дистрибутивности: $(a + b)c = ac + bc$.

Примечание 1. Если для умножения выполняется закон коммутативности, то кольцо называется *коммутативным*.

Определение 5. Если кольцо обладает левым единичным элементом $e: ex = x$ для всех x и одновременно – правым единичным элементом $e': xe' = x$ для всех x , то оба эти элемента должны быть равны, так как $e = ee' = e'$. При этих условиях элемент называют просто единичным элементом или единицей и говорят о *кольце с единицей*.

Определение 6. Если в кольце нет делителей нуля, отличных от самого нуля, т. е. если из $ab = 0$ следует, что или $a = 0$, или $b = 0$, то говорят о кольце без делителей нуля. Если, кроме того, кольцо коммутативно, то оно называется *целостным*.

Определение 7. Кольцо P называется *полем*, если для любых элементов a и b из P , из которых b отлично от нуля, существует P такой элемент q , притом, лишь единственный, который удовлетворяет равенству $bq = a$. Элемент q называется *частным* элементов a и b и обозначается символом $q = \frac{a}{b}$.

1.2. Алгебраические элементы колец

Определение 8. Элемент кольца R называется *идемпотентным* элементом, если $e^2 = e$.

0 - всегда идемпотентный.

Определение 9. Кольцо R называется *нильпотентным*, если существует такое натуральное число n , для которого произведение любых n элементов кольца равно нулю.

Пример 1. Любую абелеву группу G можно рассматривать как нильпотентное кольцо, положив $ab = 0$ для любых элементов a и b из G .

Определение 10. Пусть $(R, +, \cdot)$ – ассоциативное кольцо и k – натуральное число. Тогда k – ой степенью кольца R назовем множество $R^k = [(R, \cdot)^k]$.

Из данного определения следует, что R^k – множество, состоящее из всевозможных конечных сумм элементов, каждый из которых есть произведение не менее, чем k сомножителей. Кроме того, если R содержит единицу e , то $R^k = R$. Действительно, для любого $r \in R$ $rr = r \cdot \underbrace{e \cdots e}_{k-1} \in R^k$.

Пусть R – нильпотентное кольцо. Наименьшее натуральное число n , для которого $R^n = 0$, называется *индексом нильпотентности кольца R* . Обозначение $\text{ind } R$. Очевидно, что $\text{ind } R = 1$ тогда и только тогда, когда $R = 0$. Если $\text{ind } R = 2$, то будем называть R *кольцом с нулевым умножением*.

Определение 11. Элемент a кольца R называется *алгебраическим*, если существует многочлен в положительной степени $f(x)$ с целыми коэффициентами, то есть $F(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x, f(a) = 0$.

1.3. Пирсовские разложения колец

Пусть R – коммутативное кольцо, e – нулевой идемпотентный элемент. Определим два множества:

1. $eR = \{ex | x \in R\} \neq \emptyset$
2. $(1 - e)R = \{x - ex | x \in R\} \neq \emptyset$

Докажем, что eR и $(1 - e)R$ – подкольца в R .

Доказательство: по признаку подкольца (применим к непустым подмножествам).

1. $\forall a, b \in S, ((a - b) \in S)$;
2. $\forall a, b \in S, (ab \in S)$.

Пусть $S = eR, a = ex_1, b = ex_2$.

1. $a - b = e(x_1 - x_2) \in eR$;
2. $ab = ex_1 ex_2 = e^2 x_1 x_2 = e(ex_1 x_2) \in eR$.

Пусть $S = (1 - e)R, a = (1 - e)x_1, b = (1 - e)x_2$.

$$1. a - b = x_1 - x_2 - e(x_1 - x_2) = (1 - e)(x_1 - x_2) \in (1 - e)R;$$

$$2. ab = (1 - e)x_1(1 - e)x_2 = (1 - e)((1 - e)x_1x_2) \in (1 - e)R.$$

Докажем, что $eR + (1 - e)R = R$.

Пусть $x \in R$. Тогда $x = ex + (1 - e)x = ex + x - ex = x$.

Значит, $R \subseteq eR + (1 - e)R$. Так как $eR, (1 - e)R \subseteq R$, то $eR + (1 - e)R = \{ex + (1 - e)y = ex + y - ey | x, y \in R\} \subseteq R$.

Убедиться в том, что $eR \cap (1 - e)R = \{0\}$.

Пусть $a \in eR \cap (1 - e)R$. Тогда существуют $x, y \in R$ такие, что

$$a = ex = (1 - e)y$$

$$ea = e(ex) = e(1 - e)y = e(y - ey) = ey - ey = 0$$

Получаем $a = 0$.

Обозначим: $eR + (1 - e)R = eR \oplus (1 - e)R$ – прямая сумма двух подколец.

Таким образом, имеем $R = eR \oplus (1 - e)R$ – пирсовское разложение коммутативного кольца R по идемпотенту e .

Для любых $a \in eR$, $ea = a$, e – единичный элемент в подкольце. Для любого $c \in (1 - e)R$, $ec = 0$.

Значит, если $x \in eR$, а $y \in (1 - e)R$, то $e(x + y) = x$, получаем $xy = 0$.

Пусть R – некоммутативное кольцо, e – идемпотентный элемент.

Тогда, если e – не единица, то имеет место двустороннее пировское разложение: $R = eRe \oplus eR(1 - e) \oplus (1 - e)Re \oplus (1 - e)R(1 - e)$,

$$eRe \in a, eR(1 - e) \in b, (1 - e)Re \in c, (1 - e)R(1 - e)d,$$

$$ba = 0, ab \in eR(1 - e),$$

$$ac = 0, ca \in (1 - e)Re,$$

$$ad = da = 0,$$

$$b^2 = 0, c^2 = 0.$$

1.4. Понятие алгебры над полем

Определение 12. Алгеброй над полем P называется множество A , на котором определены две бинарные операции $+$ и \cdot , а также операция умножения элементов из P на элементы из A (то есть отображение $P \times A \rightarrow A$), удовлетворяющие следующим условиям:

1. $(A, +, \cdot)$ – кольцо;
2. $(A, +)$ – векторное пространство над полем P ;
3. $\forall \alpha \in P \forall a, b \in A (\alpha a)b = \alpha(ab) = a(\alpha b)$.

Пример 2. Пусть V – n -мерное векторное пространство над полем F и $\Phi_n(F)$ – множество всех линейных преобразований пространства V . Известно, что $\Phi(F)$ – алгебра над полем F относительно следующих операций:

1. $\forall \phi, \psi \in \Phi_n(F) \forall v \in V (\phi + \psi)(v) = \phi(v) + \psi(v)$;
2. $\forall \phi, \psi \in \Phi_n(F) \forall v \in V (\phi \cdot \psi)(v) = \psi(\phi(v))$;
3. $\forall \phi \in \Phi_n(F) \forall \alpha \in F (\alpha \phi)(a) = \alpha(\phi(a))$.

1.5. Алгебра матриц над конечным полем

Определение 13. Пусть A – алгебра над полем P . Назовем алгебру A конечномерной, если A , как векторное пространство над полем P , конечномерно. При этом размерность векторного пространства A над P будем называть размерностью или рангом алгебры A .

Пример 3. Пусть $A = C$, $P = R$. Тогда числа $1, i$ образуют базис C над R и потому $\dim C = 2$.

Пример 4. Базис алгебры $M_n(F)$ образуют матричные единицы $E_{ij} = (e_{ij})$, где $e_{ij} = 0$, если $i \neq j$ и $e_{ij} = 1$, если $i = j$. Следовательно, $\dim M_n(F) = n^2$.

1.6. Понятие подалгебры. Признак подалгебры

Определение 14. Подмножество S алгебры A над полем P назовем *подалгеброй алгебры A* , если относительно операций, определенных в A , S само является алгеброй над полем P .

Теорема 3 (Признак подалгебры). *Непустое подмножество S алгебры A над полем P тогда и только тогда является подалгеброй в A , когда выполнены следующие условия:*

1. $\forall a, b \in S \quad a - b \in S$;
2. $\forall a, b \in S \quad a \cdot b \in S$;
3. $\forall \alpha \in P \quad \forall a \in S \quad \alpha a \in S$.

Доказательство. Пусть S – подалгебра алгебры A . Тогда очевидно, что условия 1) – 3) выполнены. Обратно: пусть выполнены условия 1) – 3). Тогда из выполнимости условий 1) и 2) следует, что S – подкольцо кольца A , а из выполнимости условий 1) и 3) следует, что S – векторное подпространство пространства A . Условие 3) определения 1. выполняется в S , так как оно выполняется в A . Таким образом, S – подалгебра алгебры A .

1.7. Изоморфизм алгебр

Определение 15. Пусть A и A' – алгебры над полем P . *Изоморфизмом алгебры A на алгебру A'* назовем биективное отображение φ множества A на множество A' , удовлетворяющее следующим условиям:

1. $\forall a, b \in A \quad \varphi(a + b) = \varphi(a) + \varphi(b)$;
2. $\forall a, b \in A \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$;
3. $\forall \alpha \in P \quad \forall a \in A \quad \varphi(\alpha a) = \alpha(\varphi(a))$.

Замечание 1. Из условий 1) и 2) следует, что изоморфные алгебры являются изоморфными кольцами, а из условий 1) и 3) следует, что изоморфные алгебры являются изоморфными векторными пространствами. Поэтому изоморфизмы алгебр над полем обладают всеми свойствами изоморфизмов колец и векторных пространств.

Теорема 4. Любая алгебра с единицей ранга n над полем P изоморфна некоторой подалгебре алгебры $M_n(P)$.

Доказательство. Пусть A – алгебра ранга n над полем P . Для любого элемента a из A определим отображение $\varphi_a: A \rightarrow A$ следующим образом: $\forall x \in A \varphi_a(x) = xa$ и докажем, что φ_a – линейное отображение. Действительно,

1. $\forall x, y \in A \varphi_a(x + y) = (x + y)a = xa + ya = \varphi_a(y);$
2. $\forall x \in A \forall \alpha \in P \varphi_a(\alpha x) = (\alpha x)a = \alpha(xa) = \alpha(\varphi_a(x)).$

Заметим, что $\varphi_{a+b} = \varphi_a + \varphi_b; \varphi_{ab} = \varphi_a \varphi_b; \varphi_{\alpha a} = \alpha \varphi_a$.

Зададим теперь отображение $\gamma: A \rightarrow \Phi_n$ по следующему правилу: $\forall a \in A \gamma(a) = \varphi_a$ и докажем, что γ – инъективный гомоморфизм. Действительно, пусть $a, b \in A$ и $\gamma(a) = \gamma(b)$. Тогда $\varphi_a = \varphi_b$ то есть $\forall x \in A \varphi_a(x) = \varphi_b(x)$. Это значит, что $xa = xb$. Подставляя в это равенство единичный элемент e алгебры A , получим: $a = b$. Следовательно, γ – инъективное отображение.

Пусть $a, b \in A, \alpha \in P$. Тогда

1. $\gamma(a + b) = \varphi_{a+b} = \varphi_a + \varphi_b = \gamma(a) + \gamma(b);$
2. $\gamma(ab) = \varphi_{ab} = \varphi_a \varphi_b = \gamma(a)\gamma(b);$
3. $\gamma(\alpha a) = \varphi_{\alpha a} = \alpha \varphi_a = \alpha \gamma(a).$

Следовательно γ – гомоморфизм. Пусть $\gamma(A)$ – гомоморфный образ алгебры A . Тогда, во-первых, $\gamma(A) \cong A$, а во-вторых, $\gamma(A)$ – подалгебра алгебры Φ_n . Учитывая теперь то, что $\Phi_n \cong M_n(P)$, получим то, что требовалось доказать.

Теорема 5. Пусть A – произвольная алгебра ранга n над полем P . Тогда существует алгебра A^* ранга $n + 1$ с единицей над полем P , содержащая подалгебру, изоморфную алгебре A .

Доказательство. Рассмотрим множество $A^* = P \times A$ и определим на нем следующие операции:

$$\forall (\alpha, a), (\beta, b) \in A^* (\alpha, a) + (\beta, b) = (\alpha + \beta, a + b); \quad (1.1)$$

$$\forall (\alpha, a), (\beta, b) \in A^* (\alpha, a)(\beta, b) = (\alpha\beta, \alpha b + \beta a + ab); \quad (1.2)$$

$$\forall (\alpha, a) \in A^* \quad \forall \beta \in P \quad \beta(\alpha, a) = (\beta\alpha, \beta a). \quad (1.3)$$

Легко проверяется, что $(A^*, +)$ – абелева группа. Проверим выполнимость свойства дистрибутивности умножения относительно сложения:

$$\begin{aligned} \forall (\alpha, a), (\beta, b), (\omega, c) \in A^* \quad & (\alpha, a)((\beta, b) + (\omega, c)) = (\alpha, a)(\beta + \omega, b + c) \\ & = (\alpha(\beta + \omega), \alpha(b + c) + (\beta + \omega)a + a(b + c)) \\ & = (\alpha\beta + \alpha\omega, \alpha b + \alpha c + \beta a + \omega a + ab + ac) = \\ & = (\alpha\beta, \alpha b + \beta a + ab) + (\alpha\omega, \alpha c + \omega a + ac) \\ & = (\alpha, a)(\beta, b) + (\alpha, a)(\omega, c). \end{aligned}$$

Следовательно, $(A^*, +, \cdot)$ – кольцо. Кроме того, не трудно проверить, что множество A^* относительно операций (1.1) и (1.3) образует векторное пространство.

Таким образом, A^* – алгебра над полем P . Очевидно, что элемент $(1, 0)$ является единицей этой алгебры.

Определим размерность алгебры A^* . Пусть e_1, e_2, \dots, e_n – базис алгебры A (то есть базис векторного пространства A над полем P). Тогда система векторов $(1, 0), (0, e_1), (0, e_2), \dots, (0, e_n)$ алгебры A^* линейно независима над полем P . Кроме того, $\forall (\alpha, a) \in A^* \exists \alpha, \alpha_1, \dots, \alpha_n \in P \quad (\alpha, a) = \alpha(1, 0) + \alpha_1(0, e_1) + \dots + \alpha_n(0, e_n)$. Следовательно, A^* – алгебра ранга $n + 1$.

Рассмотрим теперь отображение $\gamma: A \rightarrow A^*$, определенное следующим образом: $\forall a \in A \quad \gamma(a) = (0, a)$. Легко видеть, что γ – инъективное отображение.

Пусть $a, b \in A, \alpha \in P$. Тогда

1. $\gamma(a + b) = (0, a + b) = (0, a) + (0, b) = \gamma(a) + \gamma(b);$
2. $\gamma(ab) = (0, ab) = (0, a)(0, b) = \gamma(a)\gamma(b);$
3. $\gamma(\alpha a) = (0, \alpha a) = \alpha(0, a) = \alpha\gamma(a).$

Следовательно, γ – гомоморфизм и потому алгебра A изоморфна подалгебре $\gamma(A)$ алгебры A^* .

Из теорем вытекает следующая теорема.

Теорема 6. Любая алгебра ранга n над полем P изоморфна некоторой подалгебре алгебры $M_{n+1}(P)$.

1.8. Понятие решетки. Основные свойства решеток

Самыми удобными объектами для знакомства с прикладными аспектами алгебры являются решетки. Решетки могут быть определены как упорядоченные особым образом множества, а их упорядоченность может быть изучена с помощью алгебраических методов.

Познакомимся с несколькими основными понятиями, теоремами и свойствами решеток.

Определение 16. Частично упорядоченное множество (P, \leq) называется линейно упорядоченным или цепью, если \leq – отношение линейного порядка.

Определение 17. Решеткой (или структурой) называется частично упорядоченное множество, в котором каждое двухэлементное подмножество имеет нижнюю и верхнюю грани.

Определение 18. Верхней границей подмножества S частично упорядоченного множества (P, \leq) называется элемент $a \in P$, удовлетворяющей условию $(\forall s \in S \ s \leq a)$.

Определение 19. Верхней гранью (или супремумом) подмножества S частично упорядоченного множества (P, \leq) называется наименьший элемент в множестве верхних границ подмножества S . Обозначается $\sup S$.

Определение 20. Нижней границей подмножества S частично упорядоченного множества (P, \leq) называется элемент $b \in P$, удовлетворяющей условию $(\forall s \in S \ s \geq b)$.

Определение 21. Нижней гранью (или инфинумом) подмножества S частично упорядоченного множества (P, \leq) называется наибольший элемент в множестве нижних границ подмножества S . Обозначается $\inf S$.

Определение 22. Полной решеткой называется частично упорядоченное множество, в котором каждое подмножество имеет нижнюю и верхнюю грани.

Замечание 2. Любая полная решетка содержит 0 и 1.

Можно сформулировать еще одно определение решетки.

Определение 23. Решеткой (или структурой) называется непустое множество L с определенными на нем двумя бинарными операциями \wedge и \vee , удовлетворяющими следующим условиям:

1. $\forall a \in L \ a \vee a = a, a \wedge a = a$ (идемпотентность);
2. $\forall a, b \in L \ a \vee b = b \vee a, a \wedge b = b \wedge a$ (коммутативность);
3. $\forall a, b, c \in L \ a \vee (b \vee c) = (a \vee b) \vee c, a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (ассоциативность);
4. $\forall a, b \in L \ a \vee (a \wedge b) = a, a \wedge (a \vee b) = a$ (свойства поглощения).

Свойства решеток:

1. Во всякой решетке (L, \wedge, \vee) операции объединения и пересечения удовлетворяют условию изотонности: если $x \leq y$, то $x \wedge z \leq z \wedge y$ и $x \vee z \leq z \vee y$.

Доказательство: из свойств решетки следует, что если $x \leq y$, то $x \wedge z = (y \wedge x) \wedge (z \wedge z) = (x \wedge z) \wedge (z \wedge y)$, откуда $x \wedge z \leq z \wedge y$ вследствие совместимости. Второе неравенство $x \vee z \leq z \vee y$ доказывается по принципу двойственности.

2. Во всякой решетке (L, \wedge, \vee) выполняются следующие неравенства дистрибутивности: $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$; $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$.

Доказательство: по свойству совместимости $x \wedge y \leq x$ и $x \wedge y \leq y \leq y \vee z$, откуда следует, что $x \wedge y \leq x \wedge (y \vee z)$. Также $x \wedge z \leq x$ и $x \wedge z \leq z \leq y \vee z$, откуда следует, что $x \wedge z \leq x \wedge (y \vee z)$. Таким образом, $x \wedge (y \vee z)$ является верхней гранью для $x \wedge y$ и $x \wedge z$, и значит, выполняется неравенство $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$.

По свойству совместимости $x \leq x \vee y$ и $y \wedge z \leq y \leq x \vee y$ откуда следует, что $x \vee (y \wedge z) \leq x \vee y$, также $x \leq x \vee z$ и $y \wedge z \leq z \leq$

$x \vee z$ откуда следует, что $x \vee (y \wedge z) \leq x \vee z$. Таким образом, $x \vee (y \wedge z)$ является нижней гранью для $x \vee y$ и $x \vee z$, и значит, выполняется неравенство $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$.

3. Во всякой решетке (L, \wedge, \vee) выполняется неравенство модулярности: если $x \leq z$, то $x \vee (y \wedge z) \leq (x \vee y) \wedge z$.

Доказательство: $x \leq x \vee y$ и $x \leq z$, значит, $x \leq (x \vee y) \wedge z$. Аналогично, $y \wedge z \leq y \leq x \vee y$ и $y \wedge z \leq z$. Следовательно, $y \wedge z \leq (x \vee y) \wedge z$, откуда $x \vee (y \wedge z) \leq (x \vee y) \wedge z$.

1.9. Диаграммы решеток

Определение 24. Назовем элементы a и b частично упорядоченного множества (P, \leq) *сравнимыми*, если $a \leq b$ или $b \leq a$. Будем говорить, что элемент b покрывает элемент a (обозначение $a < b$), если выполнены следующие условия:

1. $a < b$;
2. $\forall c \in P ((a \leq c) \wedge (c \leq b) \Rightarrow (c = a) \vee (c = b))$.

Для того чтобы изобразить частично упорядоченное множество (P, \leq) в виде диаграммы, примем следующие соглашения:

1. Различные элементы множества P изображаются различными точками плоскости.
2. Если $a, b \in P$ и b покрывает a , то точки, изображающие эти элементы, соединяются отрезком, причем точка, соответствующая b , располагается выше точки, соответствующей a .

Диаграмма может быть построена полностью лишь в том случае, когда частично упорядоченное множество P конечно. При построении диаграммы ее отрезки могут пересекаться в точках, не изображающих элементы множества P . Диаграмма, содержащая минимальное число таких пересечений, называется *оптимальной*, а не содержащая их совсем – *плоской*.

Рассмотрим примеры частично упорядоченных множеств и их диаграмм.

Пример 5. $P = (M, \leq)$, где $M = \{1, 2, 5, 7\}$;

Пример 6. $S = (M, |)$, где $M = \{1, 2, 3, 6, 10\}$;

Пример 7. $T = (M, |)$, где $M = \{2, 3, 4, 6, 12\}$;

Пример 8. $V = (M, |)$, где $M = \{2, 3, 5, 7\}$.

Диаграммы этих множеств представлены на Рисунок 1 а) – г).

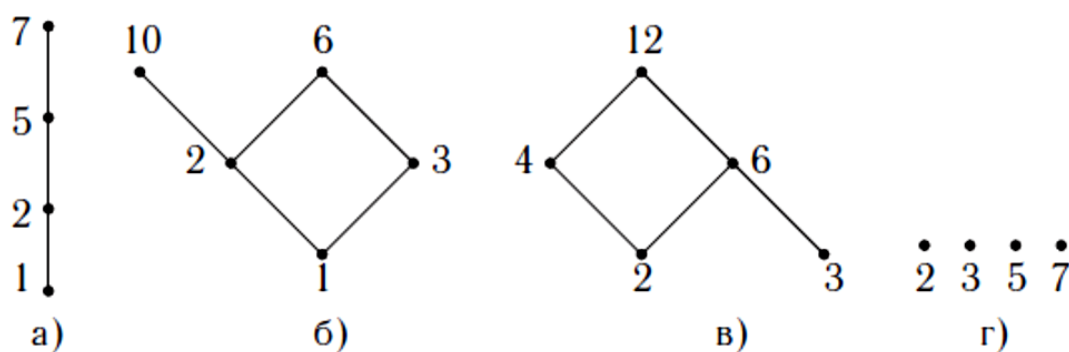


Рисунок 1

Пример 9. $U = (B(M), \subseteq)$, где $M = \{1, 2, 3\}$;

Пример 10. (M, ρ) , где $M = \{a, b, c, d, e\}$, $\rho = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (a, d), (a, e), (b, e), (c, e), (d, e)\}$;

Пример 11. (M, ρ) , где $M = \{a, b, c, d, e\}$, $\rho = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (a, d), (a, e), (b, c), (b, e), (c, e), (d, e)\}$.

Диаграммы этих множеств, представлены на Рисунок 2 а) – в).

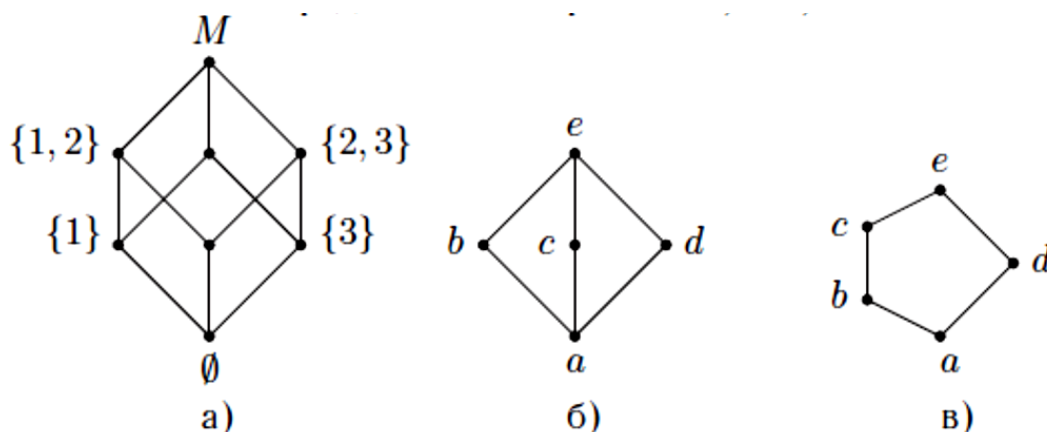


Рисунок 2

1.10. Решетка подалгебр алгебры над полем

Пусть A – алгебра над полем F . Обозначим множество всех ее подалгебр через $L(A)$ и определим на этом множестве две бинарные операции

$$\forall B, C \in L(A) B \wedge C = \{x \in A | x \in B \& x \in C\},$$

$$\forall B, C \in L(A) B \vee C = \langle B \cup C \rangle.$$

Из данных определений следует, что $B \wedge C = B \cap C$ – подалгебра алгебры A ; $B \vee C$ – наименьшая из подалгебр алгебры A , содержащая подалгебры B и C .

Теорема 7. Пусть $L(A)$ – алгебра над полем P . Тогда $(L(A), \wedge, \vee)$ – решетка.

Доказательство. Проверим выполнимость четырех аксиом решетки для $(L(A), \wedge, \vee)$.

1. Идемпотентность.

$$\forall B \in L(A) B \wedge B = B \cap B = B; B \vee B = \langle B \cup B \rangle = \langle B \rangle = B.$$

2. Коммутативность.

$$\forall B, C \in L(A) B \wedge C = B \cap C = C \cap B = C \wedge B; B \vee C = \langle B \cup C \rangle = \langle C \cup B \rangle = C \vee B.$$

3. Ассоциативность.

$$\begin{aligned} \forall B, C, D \in L(A) B \wedge (C \wedge D) &= B \cap (C \cap D) = (B \cap C) \cap D = (B \wedge C) \wedge D \\ \text{и } B \vee (C \vee D) &= B \vee \langle C \cup D \rangle = \langle B \cup \langle C \cup D \rangle \rangle = \langle B \cup (C \cup D) \rangle \\ &= \langle (B \cup C) \cup D \rangle = \langle \langle B \cup C \rangle \cup D \rangle = \langle B \cup C \rangle \vee D = (B \vee C) \vee D. \end{aligned}$$

4. Поглощение.

$$\begin{aligned} \forall B, C \in L(A) B \wedge (B \vee C) &= B \cap \langle B \cup C \rangle = B \text{ и } B \vee (B \wedge C) = \\ B \vee (B \cap C) &= B. \end{aligned}$$

ГЛАВА II. Система компьютерной алгебры GAP

2.1. Общая характеристика пакета GAP

Система GAP является свободным, открытым и расширенным пакетом программного обеспечения для вычислений в дискретной (абстрактной) алгебре. Система "расширяемая", в ней Вы можете написать свои собственные программы на языке GAP, и использовать их точно так же, как и программы, которые входят в состав системы ("библиотеки").

Разработка системы компьютерной алгебры GAP, название которой расшифровывается как "Groups, Algorithms and Programming", была начата в 1986 г. в г.Аахен, Германия. В 1997 г. центр координации разработки и технической поддержки пользователей переместился в Университет г.Сент-Эндрюс, Шотландия. В настоящее время GAP является уникальным всемирным совместным научным проектом, объединяющим специалистов в области алгебры, теории чисел, математической логики, информатики и др. наук из различных стран мира. Основные центры разработки системы находятся в университетах г.Сент-Эндрюс (Шотландия), гг. Аахен, Брауншвейг (Германия) и Университете штата Колорадо (США).

Система GAP была задумана как инструмент комбинаторной теории групп - раздела алгебры, изучающего группы, заданные порождающими элементами и определяющими соотношениями. В дальнейшем, с выходом каждой новой версии системы сфера ее применения охватывала все новые и новые разделы алгебры.

Основные особенности GAP:

- язык программирования, внешне напоминающий Паскаль;
- стандартные типы основных алгебраических объектов: групп (подстановок, абстрактных, матричных), колец, полей;
- удобные типы переменных, в т.ч. оперативно изменяемые списки и записи;

- более 4 тысяч библиотечных функций;
- обширная библиотека данных, включая практически все группы, порядок которых не превосходит 1000;
- прикладные программы, поставляемые вместе с GAP, охватывают такие разделы алгебры, как комбинаторная теория групп, конечные простые группы, теория представлений групп, теория графов, в т.ч. их группы автоморфизмов, теория кодирования, кристаллографические группы, группы Галуа и многое другое;
- подробное и удобное описание (около 1600 стр.) в формате «гипертекст»;
- бесплатное получение по сети Internet вместе с исходными текстами, являющимися незаменимым наглядным пособием для освоения GAP;
- работа в операционных системах DOS, Windows, Unix, Linux, MacOS;
- работа с процессором типа 386 и выше с ОЗУ от 8 Mb;
- занимаемое место на диске - от 10 до 100 Mb в зависимости от объема инсталляции;
- способность работать с ОЗУ до 128 Mb и файлом подкачки до 128 Mb.

Система GAP была задумана как инструмент комбинаторной теории групп – раздела алгебры, изучающего группы, заданные порождающими элементами и определяющими соотношениями. В дальнейшем, с выходом каждой новой версии системы сфера ее применения охватывала все новые и новые разделы алгебры.

GAP дает возможность производить вычисления с гигантскими целыми и рациональными числами, допустимые значения которых ограничены только объемом доступной памяти. Далее, система работает с конечными полями, многочленами от многих переменных, рациональными функциями, векторами и матрицами и многими другими функциями и списками.

2.2. Язык программирования GAP

GAP воспринимает следующие символы: цифры, буквы (верхний и нижний регистры), пробел, символы табуляции и новой строки, а также специальные символы:

" ' () * + , - # . / : ; = > ~ & [\] _ { } !

Составленные из символов слова относятся к следующим категориям:

- ключевые слова (зарезервированные последовательности букв нижнего регистра)
- идентификаторы (последовательности цифр и букв, содержащая не менее одной буквы и не являющаяся ключевым словом)
- строки (последовательности произвольных символов, заключенная в двойные кавычки)
- целые числа (последовательности цифр)
- операторы и ограничители

Следует заметить, что пробелы могут быть использованы для повышения удобочитаемости текста, так как любая последовательность пробелов воспринимается GAP как один пробел.

Ключевые слова

Ключевыми словами GAP являются следующие слова: and, do, elif, else, end, fi, for, function, if, in, local, mod, not, od, or, repeat, return, then, until, while, quit, QUIT, break, rec, continue.

Выражения

Примерами выражений являются: переменные, обращения к функциям, целые числа, перестановки, строки, функции, списки, записи. С помощью операторов из них могут быть составлены более сложные выражения. Операторы разбиты на три класса:

- операторы сравнения: =, <>, <, <=, >, >=, in;
- арифметические операторы: +, -, *, /, mod, ^;

– логические операторы: *not*, *and*, *or*.

Идентификаторы

Идентификаторы состоят из букв, цифр, символов подчеркивания *_*, и должны содержать не менее одной буквы или символа подчеркивания *_*. При этом регистр является существенным. Примеры идентификаторов: *a*, *hello*, *x100*, *foo*, *Hello*, *HELLO*, *100x*, *_100*, *MixedCase* и т.п.

2.3. Общие команды пакета

Командами в GAP называются: присваивания, вызовы процедур, структуры *if*, *while*, *repeat*, *for*, а также команда *return*. Все команды заканчиваются знаком « ; ».

1. Присваивания имеют формат:

var := expr;

2. Вызов процедуры имеют формат:

procedure – var();

procedure – var(arg – expr {, arg – expr});

Различие между процедурами и функциями введено для удобства, GAP же их не различает. Функция возвращает значение, но не производит побочных эффектов. Процедура не возвращает никакого значения, но производит какое-либо действие (например, процедуры *Print*, *Append*, *Sort*).

3. Команда *if* имеет формат:

if bool – expr1 then statements1
{ elif bool – expr2 then statements2 }
[else statements3]
fi;

При этом частей *elif* может быть произвольное количество или ни одной. Часть *else* также может отсутствовать.

4. Цикл *while* имеет формат:

while bool – expr do statements od;

Последовательность команд *statements* выполняется, пока истинно условие *bool-expr*. При этом сначала проверяется условие, а затем, если оно истинно, выполняются команды. Если уже при первом обращении условие ложно, то последовательность команд *statements* не выполнится ни разу.

5. Цикл *repeat* имеет формат:

repeat statements until bool – expr;

Последовательность команд *statements* выполняется, пока истинно условие *bool-expr*. При этом сначала выполняются команды, а затем проверяется условие. Таким образом, при любом начальном значении условия набор команд *statements* выполнится, по крайней мере, один раз.

6. Цикл *for* имеет формат:

for simple – var in list – expr do statements od;

При этом последовательность команд *statements* выполняется для каждого элемента из списка *list-expr*. Цикл *for* эквивалентен циклу *while*:

loop – list := list;
loop – index := 1;
while loop – index <= Length(loop – list) do
variable := loop – list[loop – index];
...
statements
...
loop – index := loop – index + 1;
od;

Список *list* часто является последовательностью. Команда

for variable in [from..to] do statements od;

соответствует распространенной в других языках команде

for variable from from to to do statements od;

7. Функции имеют формат:

function ([arg – ident {, arg – ident}])

```

[local loc – ident {, loc – ident} ;]
    statements
end

```

8. Команда *return* имеет формат:

```

return;
return expr;

```

Первая форма прерывает выполнение внутренней (при вызове одной функции из другой) функции и передает управление вызывающей функции, не возвращая при этом никакого значения. Вторая, кроме того, возвращает значение выражения *expr*.

2.4. Команды для вычисления в алгебрах

Таблица 1

MatAlgebra(GF(n),m)	# Построение алгебры матриц порядка m над полем, состоящим из n элементов
Elements(A)	# Элементы множества A
Dimension(A)	# Размерность алгебры A
Subalgebra(A,[m])	# Создание подалгебры алгебры A , порожденной элементом m
<u>Работа со списками и множествами:</u> N:=[]	# Создание пустого множества N
Size(N)	# Количество элементов множества N
AddSet(N,m)	# Присоединение элемента m к множеству N
Position(N,m)	# Порядок элемента m в списке N
IsSubsetSet(N,M)	# Проверяет, содержится ли каждый элемент множества M во множестве N
IntersectSet(N,M)	# Пересекает множество N с множеством M

UniteSet(N,M)	# Объединение множества N с множеством M
SubtractSet(N,M)	# Вычитает множество M от множества N , т.е. удаляет из множества M все элементы множества N
<u>Условный оператор:</u> if Q1 then P1; fi;	# Если $Q1$ - истина, то выполняется команда $P1$
if Q1 then P1; elif Q2 then A2; fi;	# Если $Q1$ - истина, то выполняется команда $P1$, а если $Q2$ - истина, то выполняется команда $P2$
<u>Работа с циклами:</u> for a in N do P; od;	# Для всех элементов множества N выполняется команда P
for i in [1..m] do P; od;	# Выполнение команды P m раз
<u>Работа с данными:</u> PrintTo(“***.dan”, N)	# Записывает данные в файл
Read(“***.dan”)	# Читает файл
quit;	# Выход из программы

ГЛАВА III. Типовая классификация подалгебр четырехмерной алгебры матриц $M(GF(2),3)$

3.1. Типы решеток подалгебр четырехмерных алгебр

В таблице 2 приведены типы решеток всех четырехмерных подалгебр в алгебре $M(GF(2),3)$. Таблица 2 получена в работе [11].

Таблица 2

№	Тип решетки	Число подалгебр в подалгебре данного типа	Количество по- далгебр данно- го типа	Количество по- далгебр данной размерности
1	(1,6,8,4,1)	20	21	497
2	(1,7,11,1,1)	21	14	
3	(1,8,12,6,1)	28	84	
4	(1,9,11,5,1)	27	42	
5	(1,9,13,4,1)	28	84	
6	(1,10,13,3,1)	28	28	
7	(1,11,17,7,1)	37	126	
8	(1,12,18,8,1)	40	84	
9	(1,12,20,9,1)	43	14	

3.2. Подалгебры, имеющие решетку типа (1, 11, 17, 7, 1)

В этом пункте на примере алгебры S_1 , имеющей решетку типа (1, 11, 17, 7, 1), демонстрируется весь процесс построения решетки подалгебр и ее диаграммы.

1. Создаем подалгебры изоморфные алгебре S_1 .

Выберем два идемпотентных элемента e_1, e_2 и два нильпотентных элемента r_1, r_2 . Зададим умножение основываясь на пирсовское разложение алгебры и найдем в алгебре A все подалгебры с заданным базисом и таблицей умножения. Составим следующую программу.

Таблица 3

Программа №1, создающая подалгебры изоморфные алгебре S_1	
eerr:=[];	# Создание каталога для размещения подалгебр
Sub:=[];b:=0;	# Создание массива sub и переменной b
ID [2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	# Массив номеров идемпотентных матриц
NI [3, 5, 7, 9, 28, 33, 37, 41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];	# Массив номеров нильпотентных матриц
A:=MatAlgebra(GF(2), 3);	# Построение алгебры матриц четвертого порядка над полем GF(2)
El:=Elements(A);	# Создание массива элементов алгебры A
Работа с циклами: for i in ID do for j in ID do for k in NI do for l in NI do	# Начало цикла построения подалгебр
Условный оператор:	#Если выполняется, то строится подалгеб-

if $j > i$ and $l > k$ and $El[i] * El[j] = El[l]$ and $El[j] * El[i] = El[l]$ and $El[i] * El[k] = El[k]$ and $El[k] * El[i] = El[l]$ and $El[i] * El[l] = El[l]$ and $El[l] * El[i] = El[l]$ and $El[j] * El[k] = El[l]$ and $El[k] * El[j] = El[k]$ and $El[j] * El[l] = El[l]$ and $El[l] * El[j] = El[l]$ and $El[l] * El[k] = El[l]$ and $El[k] * El[l] = El[l]$ then	pa B
$B := \text{Subalgebra}(A, [El[i],$ $El[j], El[k], El[l]]);$	# Записывает подалгебру алгебры A поро- жденную элементами $El[i], El[k], El[j]$ в B
$sub := \text{Elements}(B);$	# Кладем в массив sub элементы подал- гебры B
$\text{AddSet}(Sub, sub);$	#Присоединение элемента sub к массиву Sub
Условный оператор: if $\text{Size}(Sub) > b$ then $\text{Add}(eerr, [i, j, k, l]);$	# Сравниваем размер массива Sub с b. Если размер больше, то записываем в массив eerr
$b := \text{Size}(Sub);$	# Присваиваем b размер массива sub
$fi; fi;$	#Окончание работы условного оператора
$od; od; od; od;$	#Конец цикла
$\text{Sort}(eerr);$	# Упорядочиваем элементы массива eerr
$\text{PrintTo}("eerr-1.dan", "eerr:="$	#Печать результата в файл eerr-1.dan

"eerr,","","\n"," eerr =",Size(eerr),"\n");	
---	--

Результатом работы этой программы является массив, который находится в файле eerr-1.dan. Распечатаем этот файл.

eerr:= [[2, 17, 3, 5], [2, 145, 3, 7], [2, 289, 5, 7], [10, 25, 28, 37], [10, 217, 28, 64], [10, 289, 37, 64], [17, 66, 9, 41], [17, 261, 33, 41], [66, 145, 131, 456], [66, 361, 326, 456], [74, 217, 220, 439], [74, 361, 366, 439], [145, 391, 433, 505], [147, 196, 220, 366]].

Каждый элемент этого массива представляет собой четверку номеров базисных элементов алгебры. Всего получили 14 четверок, что означает, что в алгебре A содержится 14 подалгебр изоморфных подалгебре S_1 .

Для дальнейшего исследования можно выбрать любую четверку, так как у всех из них одинаковые свойства, например, возьмем [2, 17, 3, 5].

2. Вычисляем тип подалгебры.

Составим программу, которую будем использовать как функцию для вычисления типа каждой подалгебры.

Таблица 4

Программа определения типа на множестве подалгебр алгебры $M(GF(2),3)$	
tip:=function(a,b,c,d)	Задаем функцию
Local	Создаем локальные переменные
A, El, i, j, k, w, sub, tip, S, s, el, l;	Имена переменных
sub:=[];	Задаем пустой массив sub
tip:=[];	Задаем пустой массив tip
A:=MatAlgebra(GF(2),3);	Создание алгебры матриц
El:=Elements(A);	Построение массива элемен-

	ТОВ
<code>S:=Subalgebra(A,[El[a],El[b],El[c], El[d]]);</code>	Построение подалгебры
<code>for i in S do</code>	Начало цикла
<code>for k in S do</code>	Начало цикла
<code>for j in S do</code>	Начало цикла
<code>for w in S do</code>	Начало цикла
<code>s:=Subalgebra(A,[i,j,k,w]);</code>	Построение подалгебры
<code>AddSet(sub,Elements(s));</code>	Построение массива элементов и добавление его в массив sub
<code>od;</code>	Закрытие цикла
<code>od;</code>	Закрытие цикла
<code>od;</code>	Закрытие цикла
<code>for l in [1..Size(sub)] do</code>	Начало цикла
<code>Add(tip,Size(sub[l]));</code>	Добавление порядка каждого элемента в массив tip
<code>od;</code>	Закрытие цикла
<code>tip:=Collected(tip);</code>	Считаем количество элементов каждого порядка и сохраняем их в tip
<code>PrintTo("tip.txt","a= ",a,";", " b= ",b,";", " c= ",c,";", " d= ",d,"","\\n",tip);</code>	Распечатываем результаты в файл tip.txt
<code>end;;</code>	Конец функции

Запустим программу, набрав `tip(2,17,3,5);`

Программа сохраняет файл под названием `tip.txt`.

Результат имеет вид:

`a = 2; b = 17; c = 3; d = 5;`

`[[1, 1], [2, 11], [4, 17], [8, 7], [16, 1]]`

Объясним, что означает это строка:

[1, 1] – одна подалгебра порядка 1, то есть нулевая подалгебра;

[2, 11] – 11 подалгебр порядка 2;

[4, 17] – 17 подалгебр порядка 4;

[8, 7] – 7 подалгебр порядка 8;

[16, 1] – 1 подалгебра порядка 16.

Полученную последовательность пар можно переписать и в таком виде (1, 11, 17, 7, 1) – это и есть тип подалгебр.

3. Выясним отношение покрытия

Составим программу, которая определяет отношение покрытия на множестве подалгебр построенной алгебры S_1 .

Таблица 5

Программа определения отношения покрытия на множестве подалгебр алгебры $M(GF(2),3)$	
<code>pokr:=function(a,b,c,d)</code>	#Задание функции
<code>local</code>	#Задание переменных
<code>A, El, i, j, k, w, sub, tip, S, s, s1, el, l, l1, m, m1, n, n1, i1;</code>	#Имена переменных
<code>sub:=[];</code>	#Создаем массив sub
<code>for i1 in [1..9] do</code>	#Начало цикла
<code>sub[i1]:=[];</code>	#Создаем в массиве sub 9 #пустых массивов
<code>od;</code>	#Конец цикла
<code>pokr:=[];</code>	#Создание массива pokr
<code>A:=MatAlgebra(GF(2),3);</code>	#Создание алгебры
<code>El:=Elements(A);</code>	#Построение массива элементов
<code>S:=Subalgebra(A,[El[a],El[b],El[c], El[d]]);</code>	#Записывает подалгебру алгебры A порожденную элементами El[a],El[b],El[c] в S

for i in S do	#Начало цикла
for k in S do	#Начало цикла
for j in S do	#Начало цикла
for w in S do	#Начало цикла
s1:=Subalgebra(S,[i,k,j,w]);	#Записывает подалгебру алгебры S порожденную элементами i,k,j в s1
if Size(s1)=1 then	#Проверяем размер. Если равен 1
AddSet(sub[1],Elements(s1));	#Записываем в 1-й массив
fi;	#Закрываем проверку условия
if Size(s1)=2 then	#Если равен 2
AddSet(sub[2],Elements(s1));	#Записываем во 2-й массив
fi;	#Закрываем проверку условия
if Size(s1)=4 then	#Если равен 4
AddSet(sub[3],Elements(s1));	#Записываем в 3-й массив
fi;	#Закрываем проверку условия
if Size(s1)=8 then	#Если равен 8
AddSet(sub[4],Elements(s1));	#Записываем в 4-й массив
fi;	#Закрываем проверку условия
if Size(s1)=16 then	#Если равен 16
AddSet(sub[5],Elements(s1));	#Записываем в 5-й массив

fi;	#Закрываем проверку условия
if Size(s1)=32 then	#Если равен 32
AddSet(sub[6],Elements(s1));	#Записываем в 6-й массив
fi;	#Закрываем проверку условия
if Size(s1)=64 then	#Проверяем размер. Если равен 64
AddSet(sub[7],Elements(s1));	#Записываем в 7-й массив
fi;	#Закрываем проверку условия
if Size(s1)=128 then	#Если равен 128
AddSet(sub[8],Elements(s1));	#Записываем в 8-й массив
fi;	#Закрываем проверку условия
if Size(s1)=512 then	#Проверяем размер. Если равен 512
AddSet(sub[9],Elements(s1));	#Записываем в 9-й массив
fi;	#Закрываем проверку условия
od;	#Закрытие цикла
od;	#Закрытие цикла
od;	#Закрытие цикла
od;	#Закрытие цикла
for m1 in [1..Size(sub)] do	#Открытие цикла
for l1 in [1..Size(sub[m1])] do	#Открытие цикла
for n1 in [1..Size(sub[m1+1])] do	#Открытие цикла
ifIsSubset(sub[m1+1][n1],sub[#Проверяет являются ли гене-

m1][11))=true	раторы sub[m1][11] элементами sub[m1+1][n1],
Then Add(pokr,[[m1,11],[m1+1,n1]]);	#если да, то записывает в pokr
fi;	#Закрытие проверки условия
od;	#Конец цикла
od;	#Конец цикла
od;	#Конец цикла
PrintTo("pokr.txt", pokr,"\n");	#Распечатываем массив pokr в файл pokr.txt
end;;	#Конец функции

Запустим программу, набрав pokr(2,17,3,5);

Программа сохраняет файл под названием pokr.txt.

Результат имеет вид:

[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]], [[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]], [[1, 1], [2, 7]], [[1, 1], [2, 8]], [[1, 1], [2, 9]], [[1, 1], [2, 10]], [[1, 1], [2, 11]], [[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 1], [3, 4]], [[2, 2], [3, 1]], [[2, 2], [3, 5]], [[2, 2], [3, 6]], [[2, 2], [3, 7]], [[2, 2], [3, 8]], [[2, 2], [3, 9]], [[2, 3], [3, 1]], [[2, 3], [3, 10]], [[2, 3], [3, 11]], [[2, 3], [3, 12]], [[2, 4], [3, 2]], [[2, 4], [3, 5]], [[2, 4], [3, 10]], [[2, 4], [3, 13]], [[2, 4], [3, 14]], [[2, 4], [3, 15]], [[2, 5], [3, 2]], [[2, 5], [3, 6]], [[2, 5], [3, 11]], [[2, 5], [3, 16]], [[2, 6], [3, 3]], [[2, 6], [3, 5]], [[2, 6], [3, 11]], [[2, 7], [3, 3]], [[2, 7], [3, 6]], [[2, 7], [3, 10]], [[2, 7], [3, 17]], [[2, 8], [3, 4]], [[2, 8], [3, 7]], [[2, 8], [3, 13]], [[2, 8], [3, 16]], [[2, 9], [3, 4]], [[2, 9], [3, 8]], [[2, 9], [3, 12]], [[2, 9], [3, 14]], [[2, 10], [3, 7]], [[2, 10], [3, 12]], [[2, 10], [3, 15]], [[2, 10], [3, 17]], [[2, 11], [3, 9]], [[2, 11], [3, 14]], [[2, 11], [3, 16]], [[2, 11], [3, 17]], [[3, 1], [4, 1]], [[3, 1], [4, 2]], [[3, 2], [4, 1]], [[3, 2], [4, 3]], [[3, 3], [4, 1]], [[3, 4], [4, 2]], [[3, 4], [4, 3]], [[3, 5], [4, 1]], [[3, 5], [4, 4]], [[3, 5], [4, 5]], [[3, 6], [4, 1]], [[3, 6], [4, 6]], [[3, 7], [4, 2]], [[3, 7], [4, 4]], [[3, 7], [4, 6]], [[3, 8], [4, 2]], [[3, 8], [4, 5]], [[3, 9], [4, 5]], [[3, 9], [4, 6]], [[3, 10], [4, 1]], [[3, 10], [4, 7]], [[3, 11], [4, 1]], [[3, 12], [4, 2]], [[3, 12],

[4, 7]], [[3, 13], [4, 3]], [[3, 13], [4, 4]], [[3, 14], [4, 3]], [[3, 14], [4, 5]], [[3, 14], [4, 7]], [[3, 15], [4, 4]], [[3, 15], [4, 7]], [[3, 16], [4, 3]], [[3, 16], [4, 6]], [[3, 17], [4, 6]], [[3, 17], [4, 7]], [[4, 1], [5, 1]], [[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4], [5, 1]], [[4, 5], [5, 1]], [[4, 6], [5, 1]], [[4, 7], [5, 1]]]

В данном примере рассматривается подалгебра S_1 , порожденная матрицами с номерами. Эта подалгебра имеет тип $(1, 11, 17, 7, 1)$. Таким образом, все подалгебры в решетке подалгебр алгебры S_1 распределены по пяти уровням. На каждом уровне алгебры имеют двойные номера, например, номер $[2, 1]$ означает, что 2 – номер уровня, а 1 – порядковый номер подалгебры на втором уровне. Таким образом, запись $[[2, 1], [1, 1]]$ означает, что подалгебра с номером $[2, 1]$ покрывается подалгеброй с номером $[1, 1]$ в решетке подалгебр алгебры S_1 .

3. Изображение диаграмм решеток подалгебр.

Используя полученную ранее информацию, построим диаграмму решетки подалгебр алгебры S_1 (рис.3). Это будет решетка с типом $(1, 11, 17, 7, 1)$. Построение осуществим в несколько этапов.

1. Изобразим подалгебры алгебры S_1 точками (или кружочками).
2. Изобразим отношение покрытия, соединяя покрываемый элемент с покрывающим отрезком.

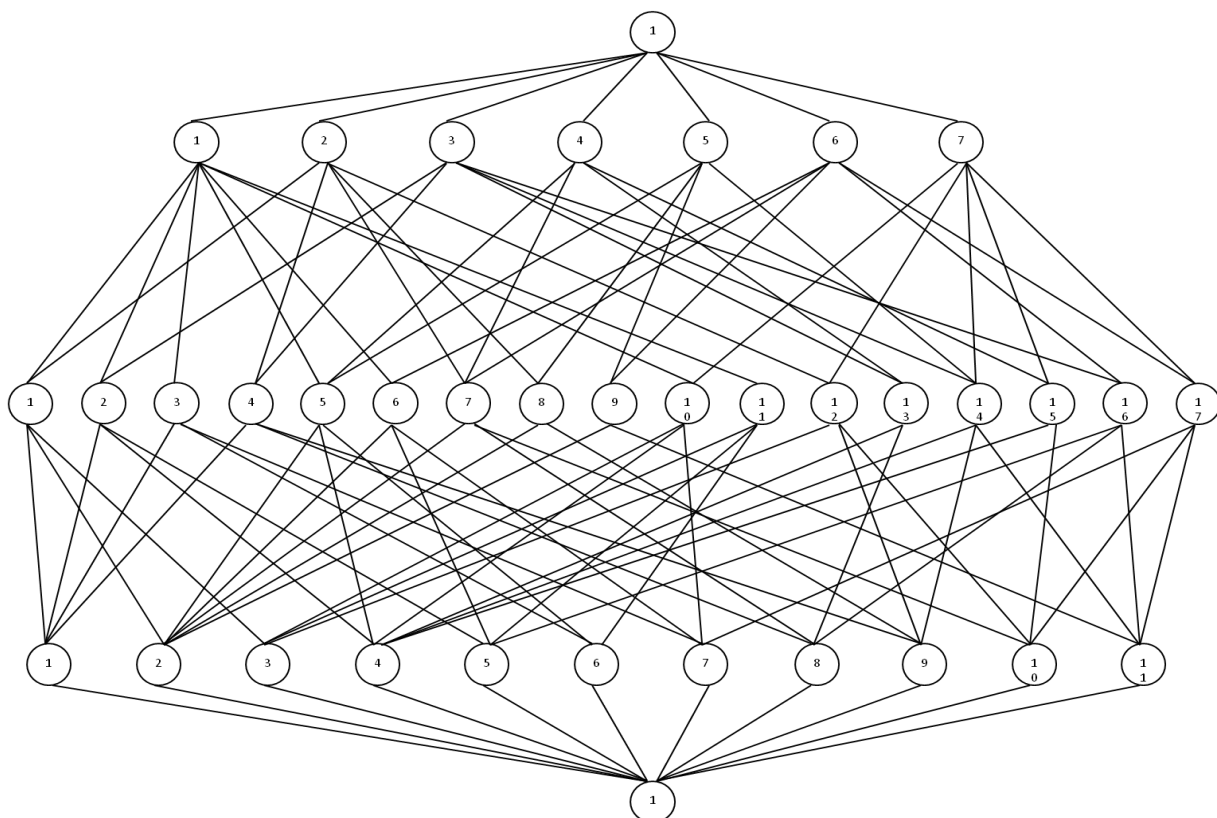


Рисунок 3

3.3. Классификация четырехмерных подалгебр в алгебре матриц третьего порядка над полем из двух элементов

Далее проводим исследование аналогичным образом и получаем таблицы со следующими результатами. Соответствующие программы и их результаты представлены в приложении № 1.

Всего было получено 4 типа, которые в свою очередь разделяются на несколько классов.

Таблица 6

№	Порождающие элементы	Определяющие соотношения					Кол-во подалгебр	Тип решетки подалгебр
1	e, r, a, a^2		e	r	a	a^2	42	(1,8,12,6,1)
		e	e	r	0	0		
		r	0	0	r	r		

		a	0	0	a^2	a		
		a^2	0	0	a	a^2		
2	e, r, a, a^2		e	r	a	a^2	42	(1,8,12,6,1)
		e	e	0	0	0		
		r	r	0	0	0		
		a	r	0	a^2	a		
		a^2	r	0	a	a^2		

Теорема 1. В алгебре A существует всего 84 подалгебры с решеткой типа $(1, 8, 12, 6, 1)$. Все эти подалгебры разбиваются на 2 подмножества, содержащих по 42 подалгебре. В каждом классе все подалгебры изоморфны между собой, а значит, имеют изоморфные решетки подалгебр, а подалгебры их различных классов – не изоморфны.

Диаграмма № 1:

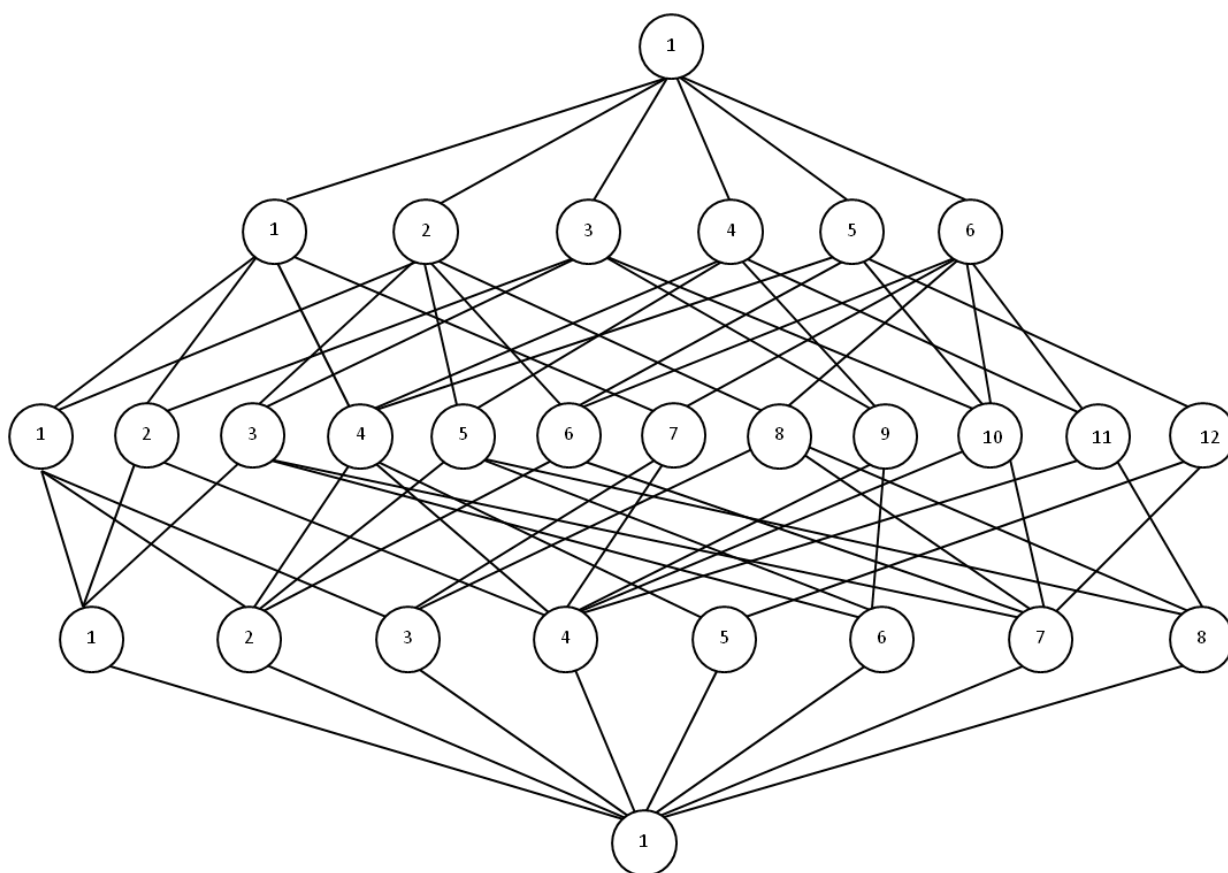


Рисунок 4

Диаграмма № 2:

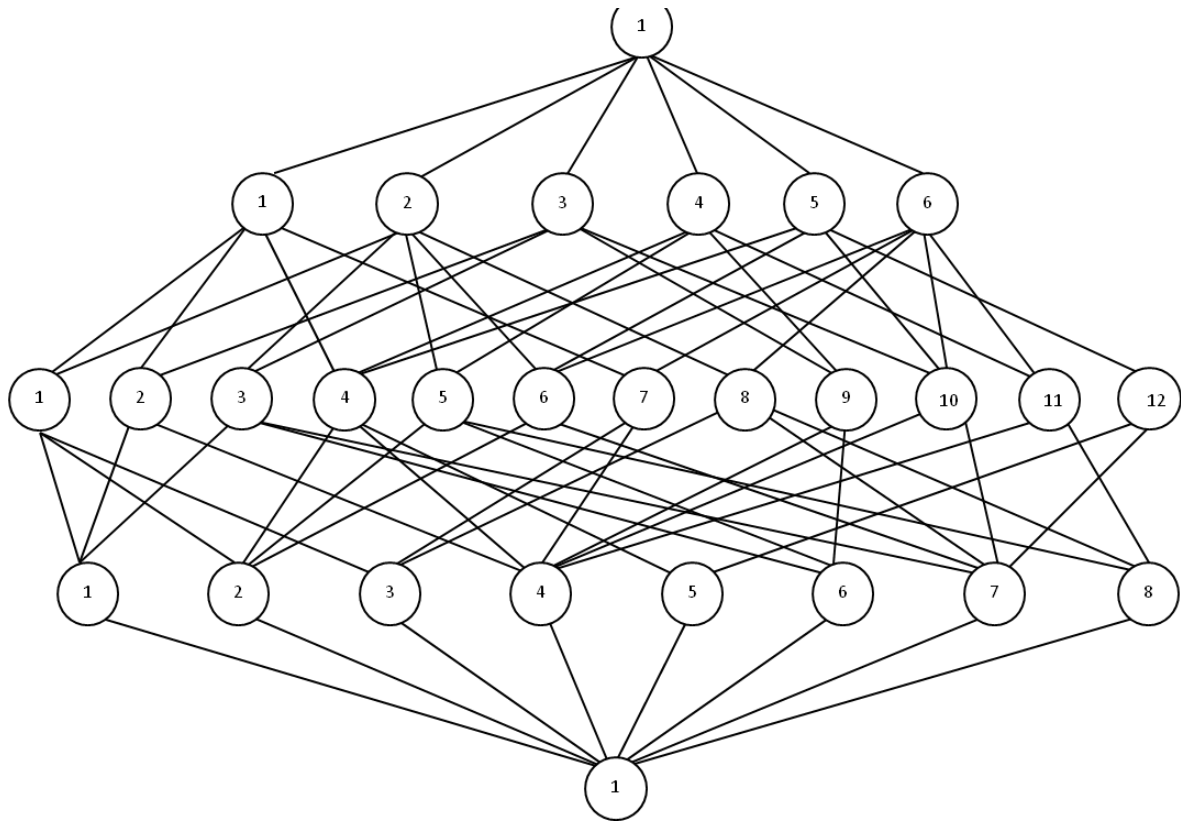


Рисунок 5

Продолжение таблицы 6

3	r_1, r_2, a, a^2		r_1	r_2	a	a^2	7	(1,7,11,1,1)
		r_1	0	0	0	0		
		r_2	0	0	0	0		
		a	r_2	$r_1 + r_2$	a^2	$a + a^2$		
		a^2	$r_1 + r_2$	r_1	$a + a^2$	a		

4	r_1, r_2, a, a^2		r_1	r_2	a	a^2	7	(1,7,11,1,1)
		r_1	0	0	r_2	$r_1 + r_2$		
		r_2	0	0	$r_1 + r_2$	r_1		
		a	0	0	$a^2 + a^2$	a		
		a^2	0	0	$a + a^2$	a		

Теорема 2. В алгебре A существует всего 14 подалгебр с решеткой типа $(1, 7, 11, 1, 1)$. Все эти подалгебры изоморфны между собой, а значит, имеют изоморфные решетки подалгебр.

Диаграмма № 3:

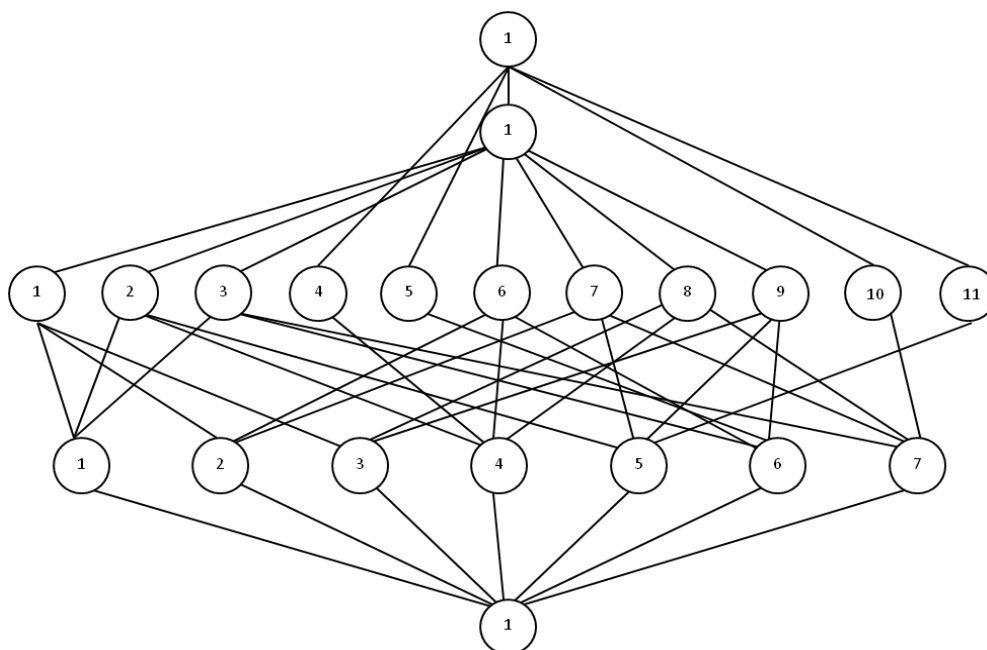


Рисунок 6

Диаграмма № 4:

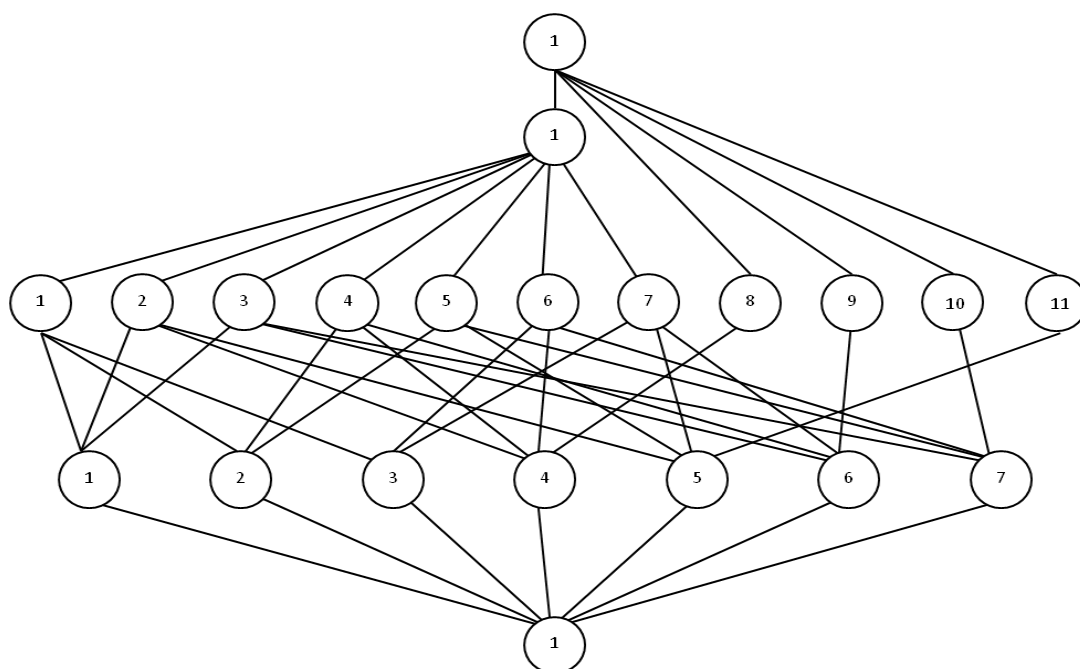


Рисунок 7

Продолжение таблицы 6

5	e_1, e_2, r_1, r_2		e_1	e_2	r_1	r_2	14	(1,11,17,7,1)
		e_1	e_1	0	r_1	r_2		
		e_2	0	e_2	0	0		
		r_1	0	r_1	0	0		
		r_2	0	0	0	0		
6	e_1, e_2, r_1, r_2		e_1	e_2	r_1	r_2	14	(1,11,17,7,1)
		e_1	e_1	0	0	0		
		e_2	0	e_2	r_1	0		
		r_1	r_1	0	0	0		
		r_2	r_2	0	0	0		
7	e_1, e_2, r_1, r_2		e_1	e_2	r_1	r_2	10	(1,12,20,9,1)
		e_1	e_1	0	r_1	r_2		
		e_2	0	e_2	0	0		
		r_1	0	r_1	0	0		
		r_2	0	r_2	0	0		

Были исследованы подалгебры с решеткой типа $(1, 11, 17, 7, 1)$. В ней 2 класса и в каждом классе по 14 подалгебр. Также исследовались подалгебры, имеющие решетку типа $(1, 12, 20, 9, 1)$. Найден 1 класс, состоящий из 10 подалгебр. Все эти подалгебры изоморфны между собой и имеют одну и ту же решетку подалгебр.

Исследование подалгебр с решетками типов $(1, 11, 17, 7, 1)$ и $(1, 12, 20, 9, 1)$ закончить не удалось.

Диаграмма № 5 и подробное исследование данного типа проведено в начале третьей главы.

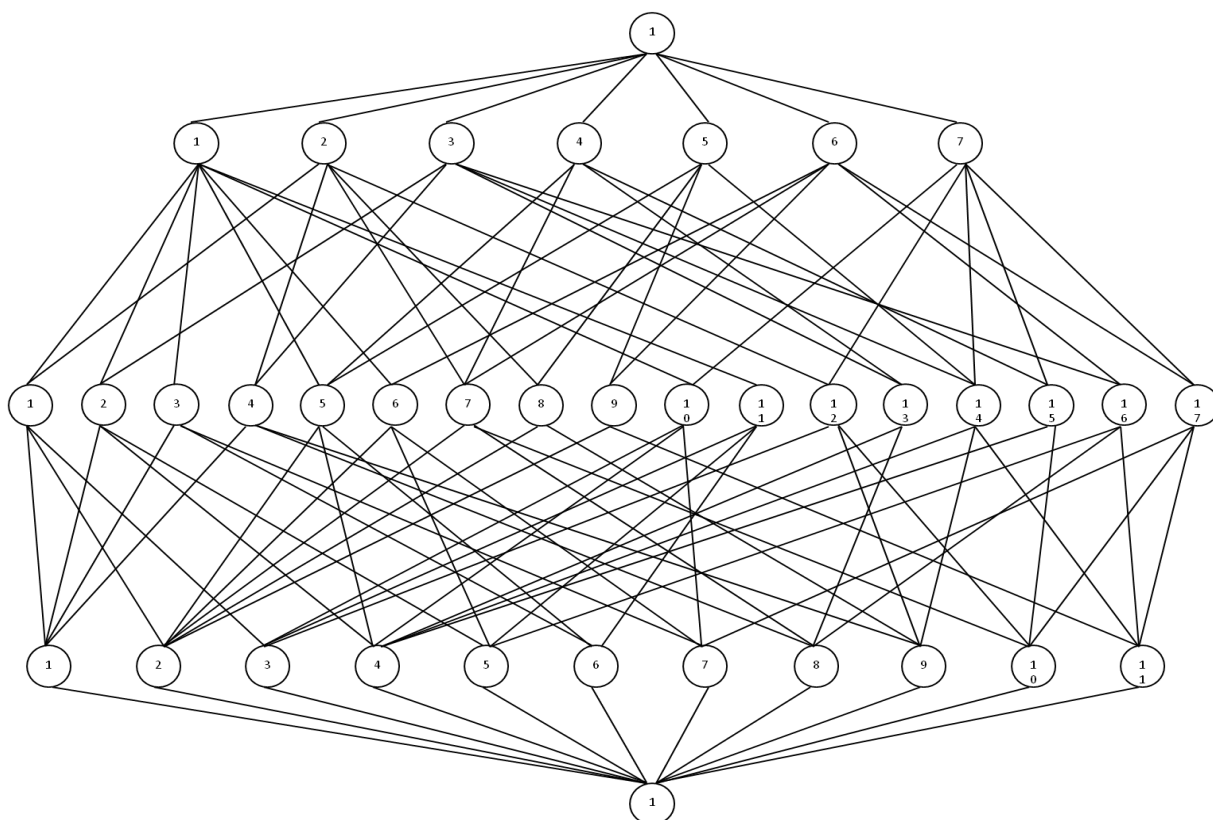


Рисунок 8

Диаграмма № 6:

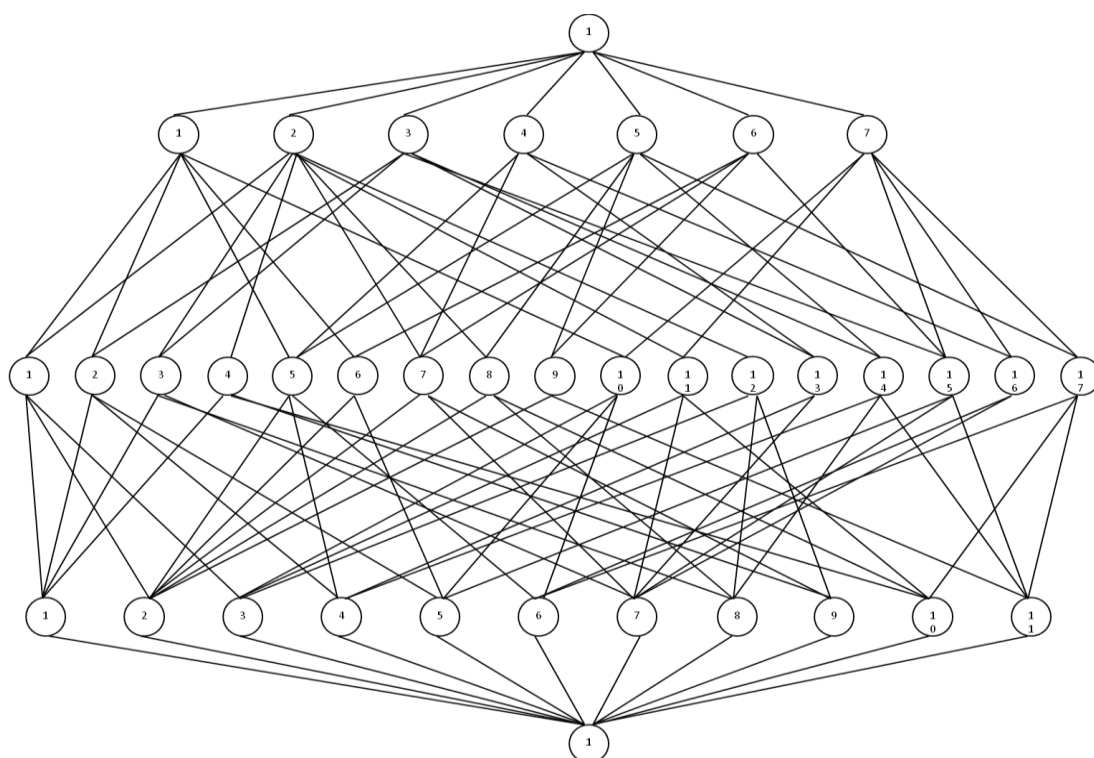


Рисунок 9

Диаграмма № 7:

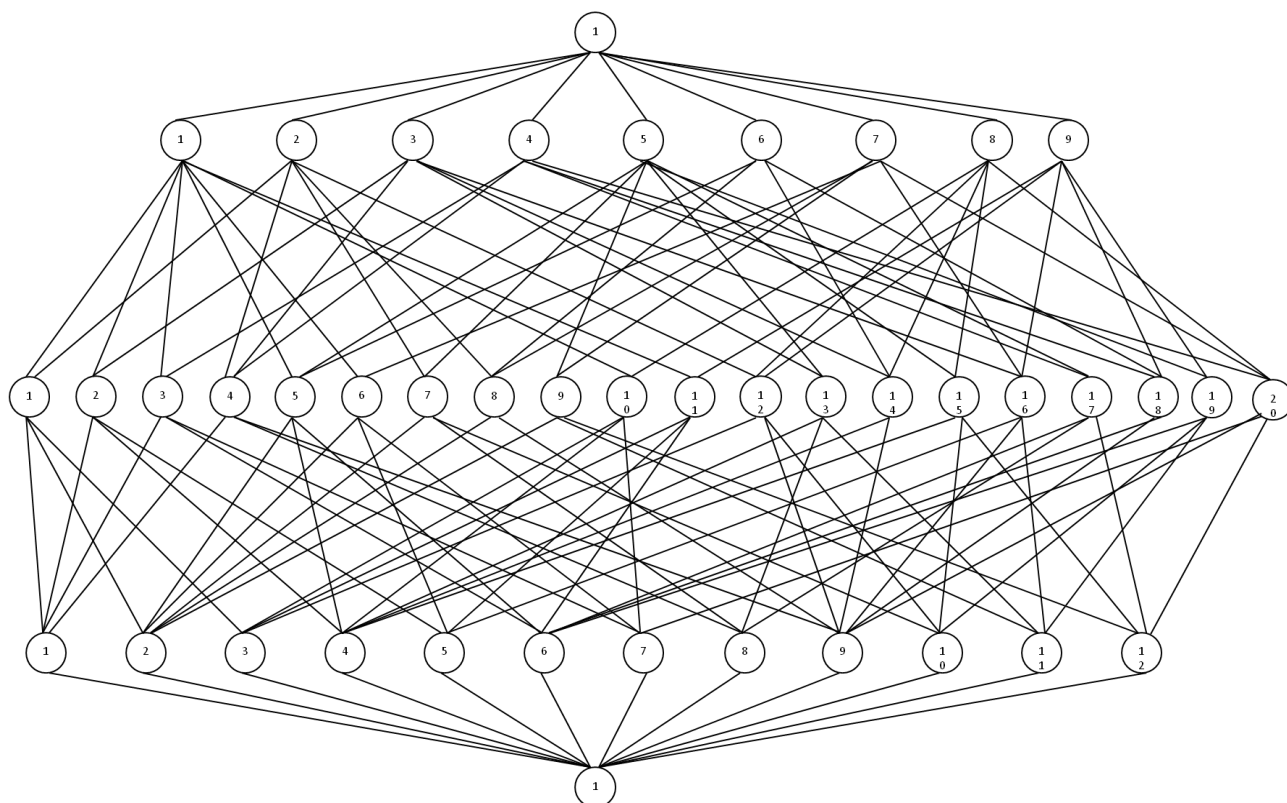


Рисунок 10

Литература

1. Ван дер Варден Б.Л. Алгебра. Под редакцией Мерзлякова Ю. И. М.: Наука, Главная редакция физико-математической литературы, 1979. - 623 с.
2. Биркгоф Г., Барти Т. К. Современная прикладная алгебра; пер. с англ. Ю. И. Манина. – Изд. 2-е, стер. – М.: Лань, 2005. – 400 с.
3. Биркгоф, Г. Теория решеток; пер. с англ. В. Н. Салий под ред. Л. А. Скорнякова. – М.: Наука, 1984. – 568 с.
4. Гантмахер Ф.Р. Теория матриц. – 4 изд. – М.: Наука. Гл. ред. физ.-мат. лит. 1988.
5. Гретцер, Г. Общая теория решеток; пер. с англ. А. Д. Больбота, В. А. Горбунова, В. И. Туманова под ред. Д. М. Смирнова. – М. : Мир, 1982. – 456 с.
6. Калужнин, Л. А. Введение в общую алгебру. – М.: Наука, 1973. – 448 с.
7. Коробков С. С. Введение в теорию решеток: Учеб. пособие по спец. курсу. Урал. гос. пед. ун-т. — Екатеринбург: Б.и., 1996. – 64с.
8. Курош А. Г. Курс высшей алгебры: Учеб. для студентов вузов по спец." Математика", "Приклад. математика". – 13-е изд., стер. – СПб.: Лань, 2004. – 432с.
9. Курош А. Г. Лекции по общей алгебре: учебник. – СПб.: Лань, 2005. – 560 с.
10. Коробков С.С. Вычисления в матричных алгебрах (Прикладные аспекты алгебры и информатики). (Рукопись). Екатеринбург, 2014.
11. Гришина А.А. Подалгебры матричной алгебры $M_3(GF(2))$. Дипломная работа. УрГПУ. Екатеринбург. 2003.
12. Barnes D.W. Lattice isomorphisms of associative algebras //J. Austral. Math. Soc. 1966. V. 6. № 1. P. 106 – 121.
13. Система компьютерной алгебры GAP – Exponenta. Режим доступа: www.exponenta.ru/soft/others/gap/1.asp
14. GAP Manual. Режим доступа: <http://www.gap-system.org/Doc/manuals.html>

Приложение 1

Приведен перечень программ, создающих подалгебры изоморфные алгебре S .

Таблица 6

Программа № 2 (соотносится с табл.6 № 6)	
eerr=[];	# Создание каталога для размещения подалгебр
Sub:=[];b:=0;	# Создание массива sub и переменной b
ID [2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	# Массив номеров идемпотентных матриц
NI [3, 5, 7, 9, 28, 33, 37, 41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];	# Массив номеров нильпотентных матриц
A:=MatAlgebra(GF(2),3);	# Построение алгебры матриц четвертого порядка над полем GF(2)
El:=Elements(A);	# Создание массива элементов алгебры A
Работа с циклами: for i in ID do for j in ID do	# Начало цикла построения подалгебр

for k in NI do for l in NI do	
Условный оператор: if j>i and l>k and El[i]*El[j]=El[1] and El[j]*El[i]=El[1] and El[i]*El[k]=El[1] and El[k]*El[i]=El[k] and El[i]*El[l]=El[1] and El[l]*El[i]=El[l] and El[j]*El[k]=El[k] and El[k]*El[j]=El[1] and El[j]*El[l]=El[1] and El[l]*El[j]=El[1] and El[l]*El[k]=El[1] and El[k]*El[l]=El[1] then	#Если выполняется, то строится подалгебра В
B:=Subalgebra(A,[El[i],El[j],El[k],El[l]]);	# Записывает подалгебру алгебры А порожденную элементамиEl[i],El[k],El[j] вВ
sub:=Elements(B);	# Кладем в массив sub элементы подалгебры В
AddSet(Sub,sub);	#Присоединение элемента sub к массиву Sub
Условный оператор: if Size(Sub) > b then Add(eerr,[i,j,k,l]);	# Сравниваем размер массива Subс b. Если размер больше, то записываем в массив eerr
b:=Size(Sub);	# Присваиваем b размер массива sub
fi;fi;	#Окончание работы условного оператора

od; od; od; od;	#Конец цикла
Sort(eerr);	# Упорядочиваем элементы массива eerr
PrintTo("eerr- 2.dan","eerr:= ",eerr,";", "\n", " eerr =", Size(eerr), ", "\n");	#Печать результата в файл eerr-2.dan

Результат:

```
eerr:= [[2, 17, 9, 65], [2, 49, 9, 73], [2, 385, 65, 73],
[4, 19, 28, 193], [4, 55, 28, 220], [4, 385, 193, 220],
[6, 17, 41, 326], [6, 49, 41, 366], [6, 391, 326, 366],
[8, 19, 64, 456], [8, 55, 64, 505], [8, 391, 456, 505],
[17, 321, 129, 131], [49, 361, 433, 439]];
|eerr|=14
```

Таблица 7

Программа № 3 (соотносится с табл. 6 № 7)	
eerr=[];	# Создание каталога для размещения подалгебр
Sub:=[];b:=0;	# Создание массива sub и переменной b
ID [2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	# Массив номеров идемпотентных матриц
NI [3, 5, 7, 9, 28, 33, 37,	# Массив номеров нильпотентных мат-

41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];	риц
A:=MatAlgebra(GF(2),3);	# Построение алгебры матриц четвертого порядка над полем GF(2)
El:=Elements(A);	# Создание массива элементов алгебры A
Работа с циклами: for i in ID do for j in ID do for k in NI do for l in NI do	# Начало цикла построения подалгебр
Условный оператор: if j>i and l>k and El[i]*El[j]=El[l] and El[j]*El[i]=El[l] and El[i]*El[k]=El[k] and El[k]*El[i]=El[l] and El[i]*El[l]=El[l] and El[l]*El[i]=El[l] and El[j]*El[k]=El[l] and El[k]*El[j]=El[k] and El[j]*El[l]=El[l] and El[l]*El[j]=El[l] and El[l]*El[k]=El[l] and El[k]*El[l]=El[l] then	#Если выполняется, то строится подалгебра B
B:=Subalgebra(A,[El[i],El[j],El[k],El[l]]);	# Записывает подалгебру алгебры A порожденную элементами El[i], El[k], El[j] в B

sub:=Elements(B);	# Кладем в массив sub элементы подалгебры B
AddSet(Sub,sub);	#Присоединение элемента sub к массиву Sub
Условный оператор: if Size(Sub) > b then Add(eerr,[i,j,k,l]);	# Сравниваем размер массива Sub с b. Если размер больше, то записываем в массив eerr
b:=Size(Sub);	# Присваиваем b размер массива sub
fi;fi;	#Окончание работы условного оператора
od; od; od; od;	#Конец цикла
Sort(eerr);	# Упорядочиваем элементы массива eerr
PrintTo("eerr-2.dan","eerr:=", "eerr,","","\n"," eerr =",Size(eerr), ","\n");	#Печать результата в файл eerr-2.dan

Результат:

```
eerr:= [ [ 2, 273, 3, 5 ], [ 10, 281, 28, 37 ], [ 17, 258, 9, 33 ],
[ 18, 257, 5, 33 ], [ 66, 337, 131, 326 ], [ 74, 345, 220, 366 ],
[ 82, 321, 41, 326 ], [ 145, 386, 73, 433 ], [ 146, 385, 7, 433 ],
[ 210, 449, 64, 456 ] ];
|eerr|=10
```

Таблица 8

Программа № 4 (соотносится с табл. 6 № 1)	
eerr:=[];	# Создание каталога для размещения подалгебр
Sub:=[];b:=0;	# Создание массива sub и переменной b
ID [2, 4, 6, 8, 10, 17, 18,	# Массив номеров идемпотентных мат-

19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	риц
NI [3, 5, 7, 9, 28, 33, 37, 41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];	# Массив номеров нильпотентных матриц
Gen1:= [11, 15, 20, 24, 26, 30, 43, 47, 52, 56, 58, 62, 69, 71, 75, 77, 84, 85, 90, 101, 109, 114, 125, 128, 139, 148, 150, 154, 161, 162, 163, 165, 167, 168, 169, 192, 197, 199, 203, 212, 215, 218, 224, 225, 233, 234, 246, 252, 262, 264, 267, 270, 276, 278, 280, 282, 285, 292, 294, 302, 303, 305, 306, 307, 309, 310, 311, 313, 314, 322, 324, 330, 338, 339, 346, 351, 354, 362, 368, 369, 377, 390, 392, 394, 401, 402, 403, 404, 405, 407, 409, 428, 447, 450, 452, 459, 464, 465, 466,	#Алгебраические элементы

473, 488, 494, 503, 507, 509];	
A:=MatAlgebra(GF(2),3);	# Построение алгебры матриц четвертого порядка над полем GF(2)
El:=Elements(A);	# Создание массива элементов алгебры A
Работа с циклами: for i in ID do for j in Gen1 do for k in NI do	# Начало цикла построения подалгебр
Условный оператор: if El[i]*El[k]=El[k] and El[k]*El[i]=El[1] and El[k]*El[j]=El[k] and El[j]*El[k]=El[1] and El[i]*El[j]=El[1] and El[j]*El[i]=El[1] then	#Если выполняется, то строится подалгебра B
B:=Subalgebra(A,[El[i],El[k],El[j]]);	# Записывает подалгебру алгебры A порожденную элементамиEl[i],El[k],El[j] вB
sub:=Elements(B);	# Кладем в массив sub элементы подалгебры B
AddSet(Sub,sub);	#Присоединение элемента sub к массиву Sub
Условный оператор: if Size(Sub) > b then Add(eerr,[i,j,k,l]);	# Сравниваем размер массива Subс b. Если размер больше, то записываем в массив eerr
b:=Size(Sub);	# Присваиваем b размер массива sub
fi;fi;	#Окончание работы условного оператора

od; od; od; od;	#Конец цикла
Sort(eerr);	# Упорядочиваем элементы массива eerr
PrintTo("eerr- 2.dan","eerr:= ",eerr,";", "\n", " eerr =", Size(eerr) , "\n");	#Печать результата в файл eerr-2.dan

Результат:

ERAA2:= [[2, 3, 401], [2, 5, 305], [2, 7, 161], [4, 5, 311],
[4, 7, 165], [6, 3, 407], [10, 28, 473], [10, 37, 313],
[10, 64, 225], [17, 9, 322], [17, 33, 262], [17, 41, 69],
[19, 37, 264], [19, 64, 197], [25, 33, 302], [25, 41, 101],
[46, 28, 488], [49, 9, 362], [66, 131, 465], [66, 326, 377],
[66, 456, 169], [74, 220, 409], [74, 366, 369], [74, 439, 233],
[145, 73, 450], [145, 433, 392], [145, 505, 71], [147, 366, 199],
[147, 439, 390], [196, 326, 192], [196, 456, 494], [217, 433, 128],
[217, 505, 503], [257, 65, 26], [257, 129, 20], [257, 193, 11],
[261, 131, 24], [289, 73, 58], [293, 220, 47], [321, 129, 212],
[321, 193, 139], [385, 65, 218]];

|ERAA2|=42

Таблица 9

Программа № 5 (соотносится с табл. 6 № 2)	
eerr:=[];	# Создание каталога для размещения подалгебр
Sub:=[];b:=0;	# Создание массива sub и переменной b
ID [2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257,	# Массив номеров идемпотентных матриц

258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	
NI [3, 5, 7, 9, 28, 33, 37, 41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];	# Массив номеров нильпотентных матриц
Gen1:= [11, 15, 20, 24, 26, 30, 43, 47, 52, 56, 58, 62, 69, 71, 75, 77, 84, 85, 90, 101, 109, 114, 125, 128, 139, 148, 150, 154, 161, 162, 163, 165, 167, 168, 169, 192, 197, 199, 203, 212, 215, 218, 224, 225, 233, 234, 246, 252, 262, 264, 267, 270, 276, 278, 280, 282, 285, 292, 294, 302, 303, 305, 306, 307, 309, 310, 311, 313, 314, 322, 324, 330, 338, 339, 346, 351, 354, 362, 368, 369, 377, 390, 392, 394, 401, 402, 403, 404, 405, 407, 409, 428, 447, 450, 452, 459, 464, 465, 466, 473, 488, 494, 503, 507, 509];	#Алгебраические элементы
A:=MatAlgebra(GF(2),3);	# Построение алгебры матриц четвертого порядка над полем GF(2)

El:=Elements(A);	# Создание массива элементов алгебры A
Работа с циклами: for i in ID do for j in Gen1 do for k in NI do	# Начало цикла построения подалгебр
Условный оператор: if El[i]*El[k]=El[1] and El[k]*El[i]=El[k] and El[k]*El[j]=El[1] and El[j]*El[k]=El[k] and El[i]*El[j]=El[1] and El[j]*El[i]=El[1] then	#Если выполняется, то строится подалгебра B
B:=Subalgebra(A,[El[i],El[k],El[j]]);	# Записывает подалгебру алгебры A порожденную элементамиEl[i],El[k],El[j] вB
sub:=Elements(B);	# Кладем в массив sub элементы подалгебры B
AddSet(Sub,sub);	#Присоединение элемента sub к массиву Sub
Условный оператор: if Size(Sub) > b then Add(eerr,[i,j,k]);	# Сравниваем размер массива Subс b. Если размер больше, то записываем в массив eerr
b:=Size(Sub);	# Присваиваем b размер массива sub
fi;fi;	#Окончание работы условного оператора
od; od; od; od;	#Конец цикла
Sort(eerr);	# Упорядочиваем элементы массива eerr
PrintTo("eerr-	#Печать результата в файл eerr-2.dan

2.dan","eerr:= ",eerr,";","\\n"," eerr =",Size(eerr) ,"\\n");	
---	--

Результат:

ERAA2:= [[2, 9, 305], [2, 65, 401], [2, 73, 161], [4, 28, 311],
[4, 193, 403], [4, 220, 165], [6, 41, 309], [6, 326, 407],
[6, 366, 163], [8, 64, 307], [8, 456, 405], [8, 505, 167],
[10, 65, 473], [10, 73, 225], [17, 3, 262], [17, 129, 322],
[17, 131, 69], [19, 129, 452], [19, 131, 197], [25, 193, 330],
[25, 220, 101], [46, 326, 252], [46, 366, 488], [49, 7, 294],
[49, 433, 362], [49, 439, 77], [55, 433, 224], [55, 439, 509],
[57, 456, 109], [57, 505, 354], [66, 9, 377], [145, 3, 392],
[196, 28, 494], [257, 5, 20], [257, 33, 26], [257, 37, 11],
[261, 33, 62], [261, 37, 43], [289, 5, 56], [321, 41, 90],
[385, 7, 148], [449, 64, 203]];

|ERAA2|=42

Таблица 10

Программа № 6 (соотносится с табл. 6 № 3)	
eerr:=[];	# Создание каталога для размещения подалгебр
Sub:=[];b:=0;	# Создание массива sub и переменной b
NI [3, 5, 7, 9, 28, 33, 37, 41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];	# Массив номеров нильпотентных матриц
Gen:= [12, 16, 27, 31, 44, 48, 59, 63, 70, 72, 76, 78, 91, 102, 110, 119, 140, 155, 174,	#Алгебраические элементы

177, 179, 181, 183, 185, 198, 200, 204, 219, 221, 228, 241, 249, 325, 327, 333, 357, 363, 365, 372, 384, 399, 414, 417, 419, 421, 423, 425, 448, 453, 455, 480, 481, 489, 504, 508, 510];	
A:=MatAlgebra(GF(2),3);	# Построение алгебры матриц четвертого порядка над полем GF(2)
El:=Elements(A);	# Создание массива элементов алгебры A
Работа с циклами: for i in NI do for k in NI do for j in Gen do	# Начало цикла построения подалгебр
Условный оператор: if k>i and El[i]*El[k]=El[1] and El[k]*El[i]=El[1] and El[i]*El[j]=El[1] and El[k]*El[j]=El[1] and El[j]*El[i]=El[k] and El[j]*El[k]=El[i]+El[k] then	#Если выполняется, то строится подалгебра B
B:=Subalgebra(A,[El[i],El[k],El[j]]);	# Записывает подалгебру алгебры A порожденную элементамиEl[i],El[k],El[j] вB
sub:=Elements(B);	# Кладем в массив sub элементы подалгебры B
AddSet(Sub,sub);	#Присоединение элемента sub к массиву

	Sub
Условный оператор: if Size(Sub) > b then Add(eerr,[i,j,k]);	# Сравниваем размер массива Sub с b. Если размер больше, то записываем в массив eerr
b:=Size(Sub);	# Присваиваем b размер массива sub
fi;fi;	#Окончание работы условного оператора
od; od; od; od;	#Конец цикла
Sort(eerr);	# Упорядочиваем элементы массива eerr
PrintTo("eerr- 2.dan","eerr:=","eerr,",";","n"," eerr =",Size(eerr)," ","n");	#Печать результата в файл eerr-2.dan

Результат:

eerr:= [[3, 129, 325], [5, 33, 27], [7, 433, 219], [9, 65, 417],
[28, 193, 357], [41, 326, 204], [64, 456, 91]];
|eerr|=7

Таблица 11

Программа № 7 (соотносится с табл. 6 № 4)	
eerr:=[];	# Создание каталога для размещения подалгебр
Sub:=[];b:=0;	# Создание массива sub и переменной b
NI [3, 5, 7, 9, 28, 33, 37, 41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];	# Массив номеров нильпотентных матриц
Gen:= [12, 16, 27, 31, 44, 48, 59, 63, 70, 72, 76, 78, 91,	#Алгебраические элементы

102, 110, 119, 140, 155, 174, 177, 179, 181, 183, 185, 198, 200, 204, 219, 221, 228, 241, 249, 325, 327, 333, 357, 363, 365, 372, 384, 399, 414, 417, 419, 421, 423, 425, 448, 453, 455, 480, 481, 489, 504, 508, 510];	
A:=MatAlgebra(GF(2),3);	# Построение алгебры матриц четвертого порядка над полем GF(2)
El:=Elements(A);	# Создание массива элементов алгебры A
Работа с циклами: for i in NI do for k in NI do for j in Gen do	# Начало цикла построения подалгебр
Условный оператор: if k>i and El[i]*El[k]=El[1] and El[k]*El[i]=El[1] and El[j]*El[i]=El[1] and El[j]*El[k]=El[1] and El[i]*El[j]=El[k] and El[k]*El[j]=El[i]+El[k] then	#Если выполняется, то строится подалгебра B
B:=Subalgebra(A,[El[i],El[k],El[j]]);	# Записывает подалгебру алгебры A порожденную элементамиEl[i],El[k],El[j] вB
sub:=Elements(B);	# Кладем в массив sub элементы подалгебры B

AddSet(Sub,sub);	#Присоединение элемента sub к массиву Sub
Условный оператор: if Size(Sub) > b then Add(eerr,[i,j,k]);	# Сравниваем размер массива Sub с b. Если размер больше, то записываем в массив eerr
b:=Size(Sub);	# Присваиваем b размер массива sub
fi;fi;	#Окончание работы условного оператора
od; od; od; od;	#Конец цикла
Sort(eerr);	# Упорядочиваем элементы массива eerr
PrintTo("eerr-2.dan","eerr:=","eerr,",";","\\n"," eerr =",Size(eerr),"\\n");	#Печать результата в файл eerr-2.dan

Результат:

```
eerr:= [ [ 3, 5, 417 ], [ 9, 33, 325 ], [ 28, 37, 453 ], [ 65, 129, 27 ],
[ 73, 433, 63 ], [ 131, 326, 48 ], [ 220, 366, 31 ] ];
|eerr|=7
```

Приложение 2

Тип (1, 11, 17, 7, 1) из табл. 6 под № 6

Покрытие имеет вид:

[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],
[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]],
[[1, 1], [2, 7]], [[1, 1], [2, 8]], [[1, 1], [2, 9]],
[[1, 1], [2, 10]], [[1, 1], [2, 11]], [[2, 1], [3, 1]],
[[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 1], [3, 4]],
[[2, 2], [3, 1]], [[2, 2], [3, 5]], [[2, 2], [3, 6]],
[[2, 2], [3, 7]], [[2, 2], [3, 8]], [[2, 2], [3, 9]],
[[2, 3], [3, 1]], [[2, 3], [3, 10]], [[2, 3], [3, 11]],
[[2, 3], [3, 12]], [[2, 4], [3, 2]], [[2, 4], [3, 5]],
[[2, 4], [3, 13]], [[2, 4], [3, 14]], [[2, 5], [3, 2]],
[[2, 5], [3, 6]], [[2, 5], [3, 10]], [[2, 5], [3, 15]],
[[2, 6], [3, 5]], [[2, 6], [3, 10]], [[2, 6], [3, 16]],
[[2, 6], [3, 17]], [[2, 7], [3, 3]], [[2, 7], [3, 7]],
[[2, 7], [3, 11]], [[2, 7], [3, 13]], [[2, 7], [3, 15]],
[[2, 7], [3, 16]], [[2, 8], [3, 3]], [[2, 8], [3, 8]],
[[2, 8], [3, 12]], [[2, 8], [3, 14]], [[2, 9], [3, 4]],
[[2, 9], [3, 7]], [[2, 9], [3, 12]], [[2, 10], [3, 4]],
[[2, 10], [3, 8]], [[2, 10], [3, 11]], [[2, 10], [3, 17]],
[[2, 11], [3, 9]], [[2, 11], [3, 14]], [[2, 11], [3, 15]],
[[2, 11], [3, 17]], [[3, 1], [4, 1]], [[3, 1], [4, 2]],
[[3, 2], [4, 1]], [[3, 2], [4, 3]], [[3, 3], [4, 2]],
[[3, 3], [4, 3]], [[3, 4], [4, 2]], [[3, 5], [4, 1]],
[[3, 5], [4, 4]], [[3, 5], [4, 5]], [[3, 6], [4, 1]],
[[3, 6], [4, 6]], [[3, 7], [4, 2]], [[3, 7], [4, 4]],
[[3, 7], [4, 6]], [[3, 8], [4, 2]], [[3, 8], [4, 5]],
[[3, 9], [4, 5]], [[3, 9], [4, 6]], [[3, 10], [4, 1]],

[[3, 10], [4, 7]], [[3, 11], [4, 2]], [[3, 11], [4, 7]],
[[3, 12], [4, 2]], [[3, 13], [4, 3]], [[3, 13], [4, 4]],
[[3, 14], [4, 3]], [[3, 14], [4, 5]], [[3, 15], [4, 3]],
[[3, 15], [4, 6]], [[3, 15], [4, 7]], [[3, 16], [4, 4]],
[[3, 16], [4, 7]], [[3, 17], [4, 5]], [[3, 17], [4, 7]],
[[4, 1], [5, 1]], [[4, 2], [5, 1]], [[4, 3], [5, 1]],
[[4, 4], [5, 1]], [[4, 5], [5, 1]], [[4, 6], [5, 1]],
[[4, 7], [5, 1]]

Приложение 3

Тип (1, 12, 20, 9, 1) из табл. 6 под № 7. Покрытие имеет вид:

[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],
[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]],
[[1, 1], [2, 7]], [[1, 1], [2, 8]], [[1, 1], [2, 9]],
[[1, 1], [2, 10]], [[1, 1], [2, 11]], [[1, 1], [2, 12]],
[[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 1], [3, 3]],
[[2, 1], [3, 4]], [[2, 2], [3, 1]], [[2, 2], [3, 5]],
[[2, 2], [3, 6]], [[2, 2], [3, 7]], [[2, 2], [3, 8]],
[[2, 2], [3, 9]], [[2, 3], [3, 1]], [[2, 3], [3, 10]],
[[2, 3], [3, 11]], [[2, 3], [3, 12]], [[2, 4], [3, 2]],
[[2, 4], [3, 5]], [[2, 4], [3, 10]], [[2, 4], [3, 13]],
[[2, 4], [3, 14]], [[2, 4], [3, 15]], [[2, 5], [3, 2]],
[[2, 5], [3, 6]], [[2, 5], [3, 11]], [[2, 5], [3, 16]],
[[2, 6], [3, 3]], [[2, 6], [3, 5]], [[2, 6], [3, 11]],
[[2, 6], [3, 17]], [[2, 6], [3, 18]], [[2, 6], [3, 19]],
[[2, 7], [3, 3]], [[2, 7], [3, 6]], [[2, 7], [3, 10]],
[[2, 7], [3, 20]], [[2, 8], [3, 4]], [[2, 8], [3, 7]],
[[2, 8], [3, 13]], [[2, 8], [3, 17]], [[2, 9], [3, 4]],
[[2, 9], [3, 8]], [[2, 9], [3, 12]], [[2, 9], [3, 14]],
[[2, 9], [3, 16]], [[2, 9], [3, 18]], [[2, 9], [3, 20]],
[[2, 10], [3, 7]], [[2, 10], [3, 12]], [[2, 10], [3, 15]],
[[2, 10], [3, 19]], [[2, 11], [3, 9]], [[2, 11], [3, 13]],
[[2, 11], [3, 16]], [[2, 11], [3, 19]], [[2, 12], [3, 9]],
[[2, 12], [3, 15]], [[2, 12], [3, 17]],
[[2, 12], [3, 20]], [[3, 1], [4, 1]], [[3, 1], [4, 2]],
[[3, 2], [4, 1]], [[3, 2], [4, 3]], [[3, 3], [4, 1]],
[[3, 3], [4, 4]], [[3, 4], [4, 2]], [[3, 4], [4, 3]],
[[3, 4], [4, 4]], [[3, 5], [4, 1]], [[3, 5], [4, 5]],

[[3, 5], [4, 6]], [[3, 6], [4, 1]], [[3, 6], [4, 7]],
 [[3, 7], [4, 2]], [[3, 7], [4, 5]], [[3, 8], [4, 2]],
 [[3, 8], [4, 6]], [[3, 8], [4, 7]], [[3, 9], [4, 5]],
 [[3, 9], [4, 7]], [[3, 10], [4, 1]], [[3, 10], [4, 8]],
 [[3, 11], [4, 1]], [[3, 11], [4, 9]], [[3, 12], [4, 2]],
 [[3, 12], [4, 8]], [[3, 12], [4, 9]], [[3, 13], [4, 3]],
 [[3, 13], [4, 5]], [[3, 14], [4, 3]], [[3, 14], [4, 6]],
 [[3, 14], [4, 8]], [[3, 15], [4, 5]], [[3, 15], [4, 8]],
 [[3, 16], [4, 3]], [[3, 16], [4, 7]], [[3, 16], [4, 9]],
 [[3, 17], [4, 4]], [[3, 17], [4, 5]], [[3, 18], [4, 4]],
 [[3, 18], [4, 6]], [[3, 18], [4, 9]], [[3, 19], [4, 5]],
 [[3, 19], [4, 9]], [[3, 20], [4, 4]], [[3, 20], [4, 7]],
 [[3, 20], [4, 8]], [[4, 1], [5, 1]], [[4, 2], [5, 1]],
 [[4, 3], [5, 1]], [[4, 4], [5, 1]], [[4, 5], [5, 1]],
 [[4, 6], [5, 1]], [[4, 7], [5, 1]], [[4, 8], [5, 1]],
 [[4, 9], [5, 1]]]

Приложение 4

Тип (1, 8, 12, 6, 1) из табл. 6 под № 1. Покрытие имеет вид:

[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],
[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]],
[[1, 1], [2, 7]], [[1, 1], [2, 8]], [[2, 1], [3, 1]],
[[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 2], [3, 1]],
[[2, 2], [3, 4]], [[2, 2], [3, 5]], [[2, 2], [3, 6]],
[[2, 3], [3, 1]], [[2, 3], [3, 7]], [[2, 3], [3, 8]],
[[2, 4], [3, 2]], [[2, 4], [3, 4]], [[2, 4], [3, 7]],
[[2, 4], [3, 9]], [[2, 4], [3, 10]], [[2, 4], [3, 11]],
[[2, 5], [3, 4]], [[2, 5], [3, 12]], [[2, 6], [3, 3]],
[[2, 6], [3, 5]], [[2, 6], [3, 9]], [[2, 7], [3, 3]],
[[2, 7], [3, 6]], [[2, 7], [3, 8]], [[2, 7], [3, 10]],
[[2, 7], [3, 12]], [[2, 8], [3, 5]], [[2, 8], [3, 8]],
[[2, 8], [3, 11]], [[3, 1], [4, 1]], [[3, 1], [4, 2]],
[[3, 2], [4, 1]], [[3, 2], [4, 3]], [[3, 3], [4, 2]],
[[3, 3], [4, 3]], [[3, 4], [4, 1]], [[3, 4], [4, 4]],
[[3, 4], [4, 5]], [[3, 5], [4, 2]], [[3, 5], [4, 4]],
[[3, 6], [4, 2]], [[3, 6], [4, 5]], [[3, 7], [4, 1]],
[[3, 7], [4, 6]], [[3, 8], [4, 2]], [[3, 8], [4, 6]],
[[3, 9], [4, 3]], [[3, 9], [4, 4]], [[3, 10], [4, 3]],
[[3, 10], [4, 5]], [[3, 10], [4, 6]], [[3, 11], [4, 4]],
[[3, 11], [4, 6]], [[3, 12], [4, 5]], [[4, 1], [5, 1]],
[[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4], [5, 1]],
[[4, 5], [5, 1]], [[4, 6], [5, 1]]]

Приложение 5

Тип (1, 8, 12, 6, 1) из табл. 6 под № 2

Покрытие имеет вид:

[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],
[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]],
[[1, 1], [2, 7]], [[1, 1], [2, 8]], [[2, 1], [3, 1]],
[[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 2], [3, 1]],
[[2, 2], [3, 4]], [[2, 2], [3, 5]], [[2, 2], [3, 6]],
[[2, 3], [3, 1]], [[2, 3], [3, 7]], [[2, 3], [3, 8]],
[[2, 4], [3, 2]], [[2, 4], [3, 4]], [[2, 4], [3, 7]],
[[2, 4], [3, 9]], [[2, 4], [3, 10]], [[2, 4], [3, 11]],
[[2, 5], [3, 4]], [[2, 5], [3, 12]], [[2, 6], [3, 3]],
[[2, 6], [3, 5]], [[2, 6], [3, 9]], [[2, 7], [3, 3]],
[[2, 7], [3, 6]], [[2, 7], [3, 8]], [[2, 7], [3, 10]],
[[2, 7], [3, 12]], [[2, 8], [3, 5]], [[2, 8], [3, 8]],
[[2, 8], [3, 11]], [[3, 1], [4, 1]], [[3, 1], [4, 2]],
[[3, 2], [4, 1]], [[3, 2], [4, 3]], [[3, 3], [4, 2]],
[[3, 3], [4, 3]], [[3, 4], [4, 1]], [[3, 4], [4, 4]],
[[3, 4], [4, 5]], [[3, 5], [4, 2]], [[3, 5], [4, 4]],
[[3, 6], [4, 2]], [[3, 6], [4, 5]], [[3, 7], [4, 1]],
[[3, 7], [4, 6]], [[3, 8], [4, 2]], [[3, 8], [4, 6]],
[[3, 9], [4, 3]], [[3, 9], [4, 4]], [[3, 10], [4, 3]],
[[3, 10], [4, 5]], [[3, 10], [4, 6]], [[3, 11], [4, 4]],
[[3, 11], [4, 6]], [[3, 12], [4, 5]], [[4, 1], [5, 1]],
[[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4], [5, 1]],
[[4, 5], [5, 1]], [[4, 6], [5, 1]]]

Приложение 6

Тип (1, 7, 11, 1, 1) из табл. 6 под № 3. Покрытие имеет вид:

[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],
[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]],
[[1, 1], [2, 7]], [[2, 1], [3, 1]], [[2, 1], [3, 2]],
[[2, 1], [3, 3]], [[2, 2], [3, 1]], [[2, 2], [3, 6]],
[[2, 2], [3, 7]], [[2, 3], [3, 1]], [[2, 3], [3, 8]],
[[2, 3], [3, 9]], [[2, 4], [3, 2]], [[2, 4], [3, 4]],
[[2, 4], [3, 6]], [[2, 4], [3, 8]], [[2, 5], [3, 2]],
[[2, 5], [3, 7]], [[2, 5], [3, 9]], [[2, 5], [3, 11]],
[[2, 6], [3, 3]], [[2, 6], [3, 5]], [[2, 6], [3, 6]],
[[2, 6], [3, 9]], [[2, 7], [3, 3]], [[2, 7], [3, 7]],
[[2, 7], [3, 8]], [[2, 7], [3, 10]], [[3, 1], [4, 1]],
[[3, 2], [4, 1]], [[3, 3], [4, 1]], [[3, 6], [4, 1]],
[[3, 7], [4, 1]], [[3, 8], [4, 1]], [[3, 9], [4, 1]],
[[4, 1], [5, 1]]]

Приложение 7

Тип (1, 7, 11, 1, 1) из табл. 6 под № 4. Покрытие имеет вид:

[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],
[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]],
[[1, 1], [2, 7]], [[2, 1], [3, 1]], [[2, 1], [3, 2]],
[[2, 1], [3, 3]], [[2, 2], [3, 1]], [[2, 2], [3, 4]],
[[2, 2], [3, 5]], [[2, 3], [3, 1]], [[2, 3], [3, 6]],
[[2, 3], [3, 7]], [[2, 4], [3, 2]], [[2, 4], [3, 4]],
[[2, 4], [3, 6]], [[2, 4], [3, 8]], [[2, 5], [3, 2]],
[[2, 5], [3, 5]], [[2, 5], [3, 7]], [[2, 5], [3, 11]],
[[2, 6], [3, 3]], [[2, 6], [3, 4]], [[2, 6], [3, 7]],
[[2, 6], [3, 9]], [[2, 7], [3, 3]], [[2, 7], [3, 5]],
[[2, 7], [3, 6]], [[2, 7], [3, 10]], [[3, 1], [4, 1]],
[[3, 2], [4, 1]], [[3, 3], [4, 1]], [[3, 4], [4, 1]],
[[3, 5], [4, 1]], [[3, 6], [4, 1]], [[3, 7], [4, 1]],
[[4, 1], [5, 1]]]

Приложение 8

Массив матриц алгебры $A = M_3(GF(2))$

[illegible]

59

75